



Securing Your Journey to the Cloud

Security Standards Compliance NIST SP 800-53 Revision 5

(Security and Privacy Controls for Information Systems and Organizations)

--

**Trend Micro Products
(Deep Discovery, Deep Security and TippingPoint)**

-

Version 3.2

Prepared by:

BD Pro
www.BDPro.ca

NOTE: This is a draft document prepared in anticipation of the formal release of NIST SP 800-53 Revision 5. It is provided for information purposes only and will be updated and amended by Trend Micro as required when the final version of Revision 5 becomes publicly available.

Security and Privacy Controls for Federal Information Systems and Organizations - NIST SP 800-53 Revision 5

Security Standards Compliance: Trend Micro Products (Deep Discovery, Deep Security and TippingPoint)

- References:
- A. Federal Information Security Management Act, (FISMA) 2002
 - B. Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Rev. 5, Initial Public Draft, August 2017
 - C. Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, NIST SP 800-53A, Rev. 4, December 2014
 - D. Security Categorization and Control Selection for National Security Systems, CNSS Instruction 1253, 27 March 2014
 - E. National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products No. 11 (CNSSP #11), 10 June 2013
 - F. FedRAMP Security Controls Baseline (for Low, Moderate and High impact systems). Rev 4, 26 January 2015
 - G. Protecting Controlled Unclassified Information in Non-federal Systems and Organizations, NIST SP-800-171, Rev. 1, 20 February 2018
 - H. Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82, Rev. 2, May 2015
 - I. ISO / IEC 15408, Common Criteria for Information Technology Security Evaluation, Ver. 3.1, Release 5, April 2017
 - J. Security Standards Compliance, SP 800-53 Rev.4 –Trend Micro Products (Deep Security, Deep Discovery Inspector and SecureCloud), Ver. 2.0, Prepared by BD Pro, February 2015
 - K. Deep Discovery Inspector v3.2, Common Criteria EAL-2 Certification Report, v1.0, 21 January 2014; and Security Target, v2.2, 20 January 2013
 - L.. Deep Security v9.5, Common Criteria EAL-2 Certification Report, 1.0, 27 March 2015; and Security Target, v21.0, 13 March 2015
 - M. TippingPoint v3.8.2, Common Criteria EAL-3 C055 Certification Report, v1, 9 March 2015; M005 Maintenance Report, 21 July 2016 and Security Target, v2.2, 21 June 2016

1. Introduction

This document is an update to the 2015 whitepaper (reference J) and considers new controls introduced in the “*Initial Public Draft*” of NIST SP 800-53 Revision 5 (reference B) and includes TippingPoint in the compliance analysis. There are two related sections in this paper:

1. Introduction – The target audience of the introduction are the senior management teams of the organizations and government agencies required to comply with FISMA requirements; and
- 2 NIST SP 800-53 Controls / Trend Micro Solution Compliancy – The target audience of the detailed compliancy table are the relevant management, security architects, technical and security risk management staff within these enterprises.

The FISMA Implementation Project includes development and promotion of key security standards and guidelines to support the implementation of and compliance of US government agencies with FISMA, addressing: (1) Categorizing information and information systems by mission impact; (2) Minimum security requirements; (3) Selecting appropriate security controls; (4) Guidance for assessing security controls and determining security control effectiveness; (5) Guidance for the security authorization of information systems; and (6) Monitoring the security controls and the security authorization of systems.

The key security standard and guidance document being used for FISMA implementation and compliance is NIST SP 800-53 Revision 5. The ultimate objective of this revision is “*make the information systems we depend on more penetration resistant to attacks; limit the damage from attacks when they occur, and make the systems resilient and survivable*”.

1.1 Trend Micro solutions & SP 800-53 compliancy – an Overview

The Trend Micro products Deep Discovery Inspector v5, Deep Security v11 and TippingPoint v3.8.2 help satisfy the requirements of NIST SP 800-53, at both the application/system enterprise level and as security features specific to the products, such as product access controls, audit capability, etc. The appropriate context of each compliancy statement is indicated in the attached compliancy table:

“**E**” - how the Trend Micro products help satisfy the Enterprise level security requirements; and

“**P**” - how the Trend Micro products satisfy the Product level security requirements. These product-specific compliancy details are needed by managers, security systems engineers and risk analysts in order that they may select and architect cost-effective secure solutions that will protect their Enterprise systems and sensitive information assets from the modern hostile threat environment.

Common Criteria Security Targets identify functional and assurance requirements to be addressed by security products in the CC evaluations. SP 800-53 (Table I-3) “*provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53*.” Such mappings indicates which evaluated CC controls will assist in supporting a product’s compliance to specific SP 800-53 controls. Based

on these mappings, the “P” context compliancy statements include those related to the SFRs and SARs used in most recent CC evaluations: Deep Discovery Inspector v3.1 – EAL 2; Deep Security v9.5 – EAL 2; and TippingPoint v3.8.2 – EAL 3.

In addition, the three Trend Micro Security Targets (references K, L and M) include “extended functions” which are relevant security requirements not found in the Common Criteria. These additional CC evaluation requirements (related to Anti-virus Requirements and Intrusion Detection System Requirements) are included in the SP 800-53 compliancy analysis of Deep Security, Deep Discovery Inspector and TippingPoint.

The SP 800-53 compliancy analysis also recognized that TippingPoint cryptographic capabilities were developed using FIPS 140-2 Level 1 evaluated libraries ¹ and that Deep Security has been validated under the FIPS 140-2 Level 1 program ^{2 3}.

Security products acquired by the US Government agencies for National Security Systems are required to have Common Criteria certification in accordance with CNSSP #11. TippingPoint v3.8.2 and related subsystems have been evaluated under the Defence Information Systems Agency (DISA) Joint Interoperability Certification program and are included on the Department of Defence (DoD) Unified Capabilities (UC) Approved Products List (APL) for US government use.

The detailed compliancy analysis also indicates if the individual SP 800-53 security requirements are included: in CNSSI 1253 baselines for National Security Systems (Reference D); in FedRAMP baselines for Cloud Service Providers (CSP) (Reference F), in SP 800-82 baselines for Industrial Control Systems (ICS) (Reference H); and/or in SP 800-171 baselines for securing Controlled Unclassed Information (CUI) (Reference G).

Virtualized servers and cloud computing environments, are being implemented throughout government enterprises and by their CSPs. They face many of the same security challenges as their physical counterparts and additionally have to contend with a number of security concerns specific to the virtual environment such as: inter VM traffic, resource contention, blurring of system and network security boundaries, mixed trust levels, security zoning, and separation of duties. In particular, organizations need to specifically protect their sensitive information assets in the virtualized multi-tenant cloud environment where the physical storage locations are unknown to them and distributed across the cloud.

The NIST SP 800-53 standard provide a foundation of security controls for incorporating into an organization’s overall security requirements baseline for mitigating risk and improving systems and application security in their physical and virtualized environments. Many of these organizations using the NIST security requirements also have obligations to be able to demonstrate compliance with the SP 800-53 security requirements. From a security product vendor’s viewpoint, there is a need to clearly demonstrate to users of their products, how their products will, help satisfy the SP 800-53 enterprise and product specific security requirements. In this document we have indicated how SP 800-53 compliance is addressed by the Trend Micro Deep Discovery Inspector, Deep Security and TippingPoint solutions.

One of the major challenges is for government enterprises and their service providers to remain compliant with the SP 800-53 standard in the constantly changing threat environment. One objective of this Trend Micro document is to provide focused guidance on how the Trend Micro Deep Discovery Inspector, Deep Security and TippingPoint solutions can effectively help deal with these ongoing challenges. The SP 800-53 security control baselines and priorities are leveraged to provide such focus in this guidance. This Prioritized Approach identifies the applicable SP 800-53 security controls baselines (L, M and H). These details will help enterprises and their service provider partners implement a continuous improvement process to protect critical assets data against the highest risk factors and today’s escalating threats.

1.1.1 Deep Discovery

The primary Deep Discovery related security products and modules include:

Deep Discovery Inspector v5.0 with combined functionality of Virtual Analyzer (sandbox threat behavior simulation), Advanced Threat Scan Engine, APT Detection, Host Severity and Threat Management capabilities has been certified to the ISO 15408 Common Criteria EAL2 level. Deep Discovery Inspector connects to Trend Micro products and hosted services to update components by connecting to the ActiveUpdate server. Trend Micro regularly creates new component versions, and performs regular updates (signatures, patterns) to address the latest threats. Deep Discovery Inspector downloads components from the Trend Micro ActiveUpdate server.

¹ TippingPoint Crypto Core OpenSSL, FIPS 140-2 Certificate 2391, 1 December 2017; and Security Policy, v1.4, 14 November 2017

² Trend Micro Java Crypto Module, FIPS 140-2 Certificate 3140, 26 February 2018; and Security Policy, v1.1, 22 February 2018

³ Trend Micro Cryptographic Module, FIPS 140-2 Certificate 3125, 12 February 2018; and Security Policy, v1.0, 2 October 2017

Deep Discovery Email Inspector v2.6 is an email security product that uses advanced malware detection techniques and custom sandboxing to identify and block the spear phishing emails that are the initial phase of most targeted attacks. It adds a transparent email inspection layer that discovers malicious content, attachments, and URL links that pass unnoticed through standard email security.

Deep Discovery Analyser v5.8 is an open custom sandbox analysis server that enhances the malware detections capabilities of other security products. It is an open Web Services interface to allow any product or process to submit samples and obtain results. Deep Discovery Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. Deep Discovery Analyzer supports integration with Trend Micro email and web security products, and can also be used to augment or centralize the sandbox analysis of other products. The custom sandboxing environments that can be created within Deep Discovery Analyzer precisely match target desktop software configurations — resulting in more accurate detections and fewer false positives. Deep Discovery Analyzer uses YARA rules to identify malware. YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment. Provides updates for product components, including pattern files.

Virtual Analyzer, provides a secure virtualized environment used to manage and analyze suspicious network and file samples. Sandbox images allow observation of file and network behavior in a natural setting without any risk of compromising the network. Virtual Analyzer performs static analysis and behavior simulation to identify potentially malicious characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings. Virtual Analyzer performs static analysis and behavior simulation to identify potentially malicious characteristics.

Management Console, provides a built-in online management console through which users can view system status, configure threat detection, configure and view logs, run reports, administer Deep Discovery Inspector, and obtain help.

Network Content Correlation Engine is a module that implements rules or policies defined by Trend Micro. Trend Micro regularly updates these rules after analyzing the patterns and trends that new and modified viruses exhibit.

Advance Threat Scan Engine is a file-based detection-scanning engine that has true file type, multi-packed files, and IntelliTrap detection. The scan engine performs the actual scanning across the network and uses a virus pattern file to analyze the files passing through the network. The virus pattern file contains binary patterns of known viruses. Trend Micro regularly releases new virus pattern files when new threats are detected.

Network Virus Scan uses a combination of patterns and heuristics to proactively detect network viruses. It monitors network packets and triggers events that can indicate an attack against a network. It can also scan traffic in specific network segments.

Network Content Inspection Engine is a module used to scan the content passing through the network layer.

Deep Discovery Director provides centralized deployment of hot fixes and patch updated, service packs and version updates, and Virtual Analyzer images, as well as configuration replication. Deep Discovery Director is an on-premises management solution that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication of Deep Discovery products. To accommodate different organizational and infrastructural requirements, it also provides flexible deployment options such as distributed mode and consolidated mode.

Network Virus Wall Enforcer regulates access based on the security posture of endpoints.

1.1.2 Deep Security

The Deep Security 10.2 product provides, in both virtualized and physical environments, the combined functionality of a Common Criteria EAL2 validated Firewall, Anti-Virus, Deep Packet Inspection, Integrity Monitoring, Log Inspection, Role Based Access Control (RBAC) and support for multi-tenant virtual environments. It should be noted that Deep Security has been validated under FIPS 140-2 Security Level 1 evaluation and certification (#3140, and 3125). The primary Deep Security modules include:

Deep Security Manager is a centralized Web-based management console which administrators use to configure security policy and deploy protection to the enforcement components: the Deep Security Virtual Appliance and the Deep Security Agent.

Firewall Module centralizes management of server firewall policy using a bidirectional stateful firewall. Supports virtual machine zoning and prevents denial of service attacks. Provides broad coverage for all IP-based protocols and frame types as well as fine-grained filtering for ports and IP and MAC addresses.

[Anti-malware Module](#) provides both real-time and on-demand protection against file-based threats, including threats commonly referred to as malware, viruses, Trojans, and spyware. To identify threats, Anti-Malware checks files against a comprehensive threat database, portions of which are hosted on servers or kept locally as updatable patterns. Anti-Malware also checks files for certain characteristics, such as compression and known exploit code. To address threats, Anti-Malware selectively performs actions that contain and remove the threats while minimizing system impact. Anti-Malware can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified threats.

[Recommendation Scans](#) identifies known vulnerabilities. The operation scans the operating system and also installed applications. Recommendation Scans automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security signatures, engines, patterns, and rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits.

[Integrity Monitoring Module](#) detects and reports malicious and unexpected changes to files and systems registry in real time, and is available in agentless form factor. Provides administrators with the ability to track both authorized and unauthorized changes made to the instance. The ability to detect unauthorized changes is a critical component in a cloud security strategy as it provides the visibility into changes that could indicate the compromise of an instance.

[Log Inspection Module](#) provides visibility into important security events buried in log files. Optimizes the identification of important security events buried in multiple log entries across the data center. Forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving. Leverages and enhances open-source software available at OSSEC.

[Intrusion Prevention Module](#) is both an Intrusion Detections System (IDS) and an Intrusion Prevention System (IPS) which protects computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network. Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets.

[Web Reputation Module](#) protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of Web sites that users are attempting to access. The Web site's reputation is correlated with the specific Web reputation policy enforced on the computer. Depending on the Web Reputation Security Level being enforced, Deep Security will either block or allow access to the URL.

[Application Control](#) module monitors changes — “drift” or “delta” — compared to the computer’s original software. Once application control is enabled, all software changes are logged and events are created when it detects new or changed software on the file system. When Deep Security Agent detects changes, an organization can allow or block the software, and optionally lock down the computer.

1.1.3 *TippingPoint*

TippingPoint v3.8.2 has been certified to ISO 15408 Common Criteria EAL 3 augmented level. This Trend Micro product is an intrusion prevention system (IPS). The system contains all the functions needed for intrusion prevention, including Internet Protocol (IP) defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of network protocols. The primary function is to protect networks from intrusion attempts by scanning network traffic, detecting intrusion attempts, and reacting to detected intrusion attempts according to the filters and action sets with which the device is configured. The custom filters comprises rules and conditions used to detect and handle malicious network traffic. Each filter includes an action set that determines the TippingPoint response when network traffic matches conditions in a filter. The primary TippingPoint modules include:

[Security Management System](#) (SMS) provides:

- Enterprise-wide device status and behavior monitoring — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status;
- IPS networking and configuration — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group;
- Filter customization — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings; and

-
- Filter and software distribution — monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS client. The SMS client and Central Management Server can distribute these packages according to segment group settings. The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates.

Threat Insights is an aggregation portal that takes events from TippingPoint NGIPS, vulnerability scanners, and sandboxing solutions and displays them in one place to prioritize, automate, and consolidate network threat information. This allows multiple security groups to have a common framework for evaluation and resolution. By automating the aggregation of threat data from multiple security tools, Threat Insights assists security professionals by prioritizing incident response measures for breaches or potential vulnerabilities, and highlights pre-emptive actions already taken to protect a network.

Threat Suppression Engine (TSE) is a line-speed hardware engine that contains all the functions needed for Intrusion Prevention. The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The blocking of the traffic and packets ensures that the attack never reaches its destination. The combination of high-speed network processors and custom chips provides the basis for IPS technology. These highly specialized traffic classification engines enable the IPS to filter with extreme accuracy at gigabit speeds and microsecond latencies. Unlike software-based systems whose performance is affected by the number of filters installed, the highly-scalable capacity of the hardware engine allows thousands of filters to run simultaneously with no impact on performance or accuracy.

Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation. The TMC collects threat information and creates Digital Vaccine packages that are made available on the TMC website. The packages include filters that block malicious traffic and attacks on a network.

Digital Vaccine (DV) The DV filters are contained in a Digital Vaccine package. All IPS devices have a DV package installed and configured to provide out-of-the-box IPS protection for the network. The filters within the DV package are developed by TippingPoint's Digital Vaccine Labs to protect the network from specific exploits as well as potential attack permutations to address for Zero-Day threats. These filters include traffic anomaly filters and vulnerability-based filters. Vulnerability-based filters are designed to protect the network from an attack that takes advantage of a weakness in application software. For viruses that are not based on a specific vulnerability in software, the DV provides signature filters. TippingPoint delivers weekly DV updates that can be automatically installed on the IPS device. If a critical vulnerability or threat is discovered, DV updates are immediately distributed to customers.

Local Security Manager (LSM) provides a browser-based GUI for administering the IPS.

1.1.4 Related Services

These products and **other Trend Micro services** can be integrated into various enterprise architectures to effectively minimize cyber security risks. Such Trend Micro services include:

Control Manager provides a centralized management function for Deep Discovery Inspector (and other Trend Micro products) to control antivirus and other security programs.

Smart Protection Network is used to discover threats as a cloud-based protection system which combines advanced threat research with intelligence from customers to provide better protection and minimize the impact of targeted attacks.

Smart Protection Server provides the same web protection services offered by the Smart Protection Network but localizes these services to the corporate network.

Web Reputation Services - Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web Reputation Services assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

TrendLabs is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services and carries out all virus research and case analysis for Trend Micro and its customers. It designs and tests virus pattern files and refines the scan engine to keep Trend Micro technology up to date and effective against the latest threats. During virus outbreaks, TrendLabs implements strict "Red Alert" escalation procedures to notify users and produce cures as quickly as possible. Trend Micro's virus doctors usually develop an initial "fix" for a major new virus in 45 minutes or less, which can be distributed through the active updates mechanism. TrendLabs also educates users about security threats and promotes safe computing by compiling virus definitions and other useful information on the company's web site.

Threat Encyclopedia - Most malware today consists of "blended threats" - multiple attack techniques combined to bypass computer security protocols and other security controls. Trend Micro combats such complex malware with products that create a custom defense strategy. The online Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Threat Management Services provides organizations with an effective way to discover, mitigate, and manage stealthy and zero-day internal threats. Threat Management Services brings together security experts and a host of solutions to provide ongoing security services. These services ensure timely and efficient responses to threats, identify security gaps that leave the network vulnerable to threats, help minimize data loss, significantly reduce damage containment costs, and simplify the maintenance of network security.

Threat Management Service Portal is an on premise or hosted service which receives logs and data from registered products (DDI) and creates reports to enable product users to respond to threats in a timely manner and receive up-to-date information about the latest and emerging threats.

Threat Connect correlates suspicious objects detected in the organizations environment and threat data from the Trend Micro Smart Protection Network. By providing on-demand access to Trend Micro intelligence databases, Threat Connect enables an organization to identify and investigate potential threats to their environment.

Mobile App Reputation Services (MARS) collects data about detected threats in mobile devices. Mobile App Reputation Service is an advanced sandbox environment that analyzes mobile app runtime behavior to detect privacy leaks, repacked mobile apps, third-party advertisement SDKs, vulnerabilities, and app categories.

Threat Mitigator receives mitigation requests from Deep Discovery Inspector after a threat is detected. Threat Mitigator then notifies the Threat Management Agent installed on a host to run a mitigation task.

Mitigation (Module) Devices performs threat cleanup activities on network endpoints.

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides the latest downloads of virus pattern files, scan engines, and program files through the Internet. ActiveUpdate does not interrupt network services or require you to restart clients. One Agent, the Active Agent, in a network will receive updates from the ActiveUpdate Server. All other Agents (called Inactive Agents) in the network will receive updates from the Active Agent.

2. NIST SP 800-53 Requirements / Trend Micro Solution Compliancy Table

The following Compliancy Table identifies Trend Micro products and their security features which can contribute to satisfying specific SP 800-53 security control requirements and mitigating the security risks to acceptable levels. The target audience of this detailed table are the relevant management, technical and security risk management staff of organizations required to comply with FISMA and related security requirements.

Based on this analysis, the following table contains a resulting subset of the SP 800-53 controls. It is intended to be of use in the conduct of the required risk assessments and the related selection of required security measures (and security products) to help mitigate risk to critical enterprise, information and system assets.

AC-2 Access Control / Account Management

<p>AC-2 Access Control / Account Management</p> <p>a. Define and document the types of system accounts allowed for use within the system in support of organizational missions and business functions;</p> <p>b. Assign account managers for system accounts;</p> <p>c. Establish conditions for group and role membership;</p> <p>d. Specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;</p> <p>e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create system accounts;</p> <p>f. Create, enable, modify, disable, and remove system accounts in accordance with [Assignment: organization-defined policy, procedures, and conditions];</p> <p>g. Monitor the use of system accounts;</p> <p>h. Notify account managers within [Assignment: organization-defined time-period for each situation]:</p> <ol style="list-style-type: none"> 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual system usage or need-to-know changes for an individual; <p>i. Authorize access to the system based on:</p> <ol style="list-style-type: none"> 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions and business functions; <p>j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];</p> <p>k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group; and</p> <p>l. Align account management processes with personnel termination and transfer processes.</p> <p>Supplemental Guidance: System account types include, for example, individual, shared, group, system, guest, anonymous, emergency, developer/manufacturer/vendor, temporary, and service. The identification of authorized users of the system and the specification of access privileges reflects the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by appropriate organizational personnel responsible for approving such accounts and privileged access, including, for example, system owner, mission/business owner, or chief information security officer. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.</p> <p>Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account</p>	<p>LMH</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p>	<p>Deep Discovery Inspector supports Role Based Access Control with 3 user roles. It is also integrated with Active Directory supporting user and group mapping to the roles. Roles used are System Administrator, Administrators and Viewers.</p> <p>Deep Discovery Email Inspector uses role-based access control to grant and control access to the management console. This feature is used to assign specific management console privileges to accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users log on to the management console using custom user accounts.</p> <p>Deep Discovery Analyzer makes use of a role-based access control to configure 3 user roles controlling access to the management console. It is also integrated with Active Directory supporting user and group mapping to the roles.</p> <p>Deep Security solution has users, roles, and contacts that can be created and managed. Deep Security assists in meeting this requirement through the use of Role Based Access Controls. The role-based access allows multiple administrators (Users), each with different sets of access and editing rights, to edit and monitor different aspects of the system and receive information appropriate to them. Deep Security supports multi factor authentication of users. Deep Security can be synchronized Active Directory to populate the user list. Users can then sign into Deep Security Manager using the password stored in the directory. Deep Security can be configured to use SAML single sign-on, users signing in to an organization's portal can seamlessly sign in to Deep Security without an existing Deep Security account. SAML single sign-on also makes it possible to implement user authentication access control features such as:</p> <ul style="list-style-type: none"> • Password strength or change enforcement; • One-Time Password (OTP); and • Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA). <p>TippingPoint SMS makes use of Role Based Access Controls using the username, which is used to identify the role of the user and the password to authenticate them. The SMS allows custom Groups and Roles to be created. The role creation allows for granular permissions assignments. There are three roles that can be assigned to a user.</p> <p>This capability is addressed in the TippingPoint Common Criteria, Security Target requirement class FMT: Security Management and specifically FMT_SMR.1 Group Security Roles</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following control which is mapped (in SP 800-53 Table I-3) to</p>
---	--	------------	---

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts including, for example, local logon accounts used for special tasks or when network resources are unavailable. Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example, when shared/group, emergency, or temporary accounts are no longer required; or when individuals are transferred or terminated. Some types of system accounts may require specialized training. Related Controls: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-9, CM-5, IA-2, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, SC-7, SC-13, SC-37. References: NIST Special Publications 800-162, 800-178.</p>			<p>supporting the AC-2 control.</p> <ul style="list-style-type: none"> - FIA_ATD.1 (<i>Identification and Authentication / User Attribute Definition</i>).
<p>AC-2 (4) Access Control / Account Management / Automated Audit Actions</p> <p>Automatically audit account creation, modification, enabling, disabling, and removal actions, and notify [Assignment: organization-defined personnel or roles].</p> <p>Related Controls: AU-2, AU-12.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector solution satisfies this requirement through the use of Role Based Access Controls, which are audited in terms of the defined auditable events as documented in the Deep Discovery Inspector, Common Criteria, Security Target.</p> <p>Deep Discovery Email Inspector provides details about user access, policy modification, network setting changes, and other events that occurred using the Deep Discovery Email Inspector management console. Deep Discovery Email Inspector maintains two system event log types:</p> <ul style="list-style-type: none"> • Update events: All component update events; and • Audit logs: All user access events. <p>Deep Discovery Analyzer provides details about user access, policy modification, network setting changes, and other events that occurred using the Deep Discovery Analyzer management console. Deep Discovery Analyzer maintains two system event log types: Update events: All component update events and audit logs: All user access events.</p> <p>Deep Security solution satisfies this requirement through the use of Role Based Access Controls, which are audited in terms of the defined auditable events. The user and group account management data that is automatically audited as auditable events are documented in the Deep Security, Common Criteria, Security Target.</p> <p>TippingPoint - The SMS Audit log tracks all of the activity referenced in the control. The IPS Audit log also tracks all of this information. The Audit logs from SMS and IPS can automatically be delivered to any SIEM or other log management solution via Syslog. The TippingPoint IPS can configure notification contacts to send messages to a recipient (either human or machine) in response to a traffic-related event that occurs on the IPS device. The traffic-related event can be the result of triggering an IPS filter configured with an action set that specifies a notification contact. TippingPoint IPS also provides a Management Interface that enables authorized administrative users to access the security management capabilities and to view IPS data and audit data.</p>
<p>AC-2 (7) Access Control / Account Management / Role-Based Schemes</p> <p>(a) Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes allowed system access and privileges into roles;</p> <p>(b) Monitor privileged role assignments; and</p> <p>(c) Revoke access when privileged role assignments are no longer appropriate.</p> <p>Supplemental Guidance:</p> <p>Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.</p>	CNSSI FedRAMP 800-171 CUI	P	<p>Deep Discovery Inspector uses Role Based Access Control whereby each user is assigned a specific privileged management role. The role determines the management console menu items accessible to that user. Only administrators can edit and revoke accounts. Any administrator can add an account and edit or delete any other administrator account except for the system administration account. Administrators can change their account password but cannot edit or delete their own accounts.</p> <p>Deep Discovery Email Inspector uses Role-Based Access Control to grant and control access to the privileged management console. This feature is used to assign specific management console privileges to accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users log on to the management console using custom user accounts.</p> <p>Deep Discovery Analyzer makes use of Role Based Access Control for administration, the Role-based administration streamlines how administrators configure user accounts and control access to the management console.</p> <p>Deep Security uses role-based access control (RBAC) to restrict user permissions to parts of Deep Security. Access rights and editing privileges are attached to roles and not to users. Once Deep Security Manager is installed, individual accounts can be created for each user and each user can be assigned a role that will restrict their activities to all but those necessary for the completion of their duties. To change the access rights and editing privileges of an individual</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>AC-2 (7) Access Control / Account Management / Role-Based Schemes</p> <p>(... Continued.)</p>			<p>user, assign a different role to the user or edit the role. The access that roles have to computers and policies can be restricted to subsets of computers and policies. For example, users can be permitted to view all existing computers, but only permitted to modify those in a particular group.</p> <p>TippingPoint - The SMS uses capabilities and roles to give users permissions to perform specific actions within the system. A capability is an ability to affect an object in the system; for example, the ability to add a device. A role is a collection of capabilities. The SMS uses three predefined, basic roles: superuser, admin, and operator. The predefined system roles cannot be modified, but can be used as starting points to initialize new roles. When a role is created, a base system role can be selected from which to initialize the new role. The new role is given the same capabilities as the system role it is initialized from, until the capabilities are customized. New roles can be created to expand or limit the capabilities of existing roles or to target a specific set of capabilities for a group of SMS users. The access rights and capabilities of users can be further controlled through Groups. This capability is further addressed in the TippingPoint Common Criteria, Security Target requirement class FMT: Security Management and specifically FMT_SMR.1 Group Security Roles.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following control which is mapped (in SP 800-53 Table I-3) to supporting the AC-2 (7) control:</p> <ul style="list-style-type: none"> - FMT_SMR.1 (<i>Security Management / Security Management Roles / Security Roles</i>) <p>The Common Criteria EAL-2 Certification Report for Deep Discovery Inspector v3.1 includes compliance to Security Roles, through Role Based Access Controls.</p> <p>Deep Security v9.5 which is currently being evaluated to the Common Criteria EAL2 level includes compliance to Security Roles through Role Based Access Controls.</p>
<p>AC-2 (15) Access Control / Account Management / Attribute-Based Schemes</p> <p>(a) Establish and administer privileged user accounts in accordance with an attribute-based access scheme that specifies allowed system access and privileges based on attributes;</p> <p>(b) Monitor privileged attribute-based assignments;</p> <p>(c) Monitor changes to attributes; and</p> <p>(d) Revoke access when privileged attribute-based assignments are no longer appropriate.</p> <p>Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.</p>	800-171 CUI	P	<p>Deep Security Manager makes use of SAML assertions which use attribute value(s) to determine the tenant, identity provider, and role of the user. A single assertion may contain roles from multiple tenants.</p>

AC-3 Access Control / Access Enforcement

<p>AC-3 Access Control / Access Enforcement</p> <p>Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.</p> <p>Supplemental Guidance: Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in</p>	<p>L M H</p> <p>CNSSI</p> <p>FedRAMP</p> <p>800-82 ICS</p> <p>800-171 CUI</p>	P	<p>Deep Discovery Inspector enforces access to authorized product administrators' using role-based access control. All product administrators are assigned roles at creation. Authorized product administrators can only access the product through the administrative interface. They have full access to the functions permitted by their roles.</p> <p>Deep Discovery Email Inspector enforces access to authorized product administrators' using role-based access control. All product administrators are assigned roles at creation. Authorized product administrators can only access the product through the administrative interface. They have full access to the functions permitted by their roles.</p>
---	---	---	---

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.</p> <p>Related Controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-25, PS-3, SC-2, SC-3, SC-4, SC-13, SC-28, SC-31, SC-34, SI-4.</p> <p>References: NIST Special Publications 800-57-1, 800-57-2, 800-57-3, 800-162; NIST Interagency Report 7874.</p>		<p>Deep Discovery Analyzer enforces access to authorized product administrators' using role-based access control. All product administrators are assigned roles at creation. Authorized product administrators can only access the product through the administrative interface. They have full access to the functions permitted by their roles.</p> <p>Deep Security access enforcement includes Role-based access which allows multiple administrators, each with different sets of access and editing rights, to edit and monitor different aspects of the system and receive information appropriate to them. In addition, digital signatures are used to authenticate system components and verify the integrity of rules.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following controls which are mapped (in SP 800-53 Table I-3) as supporting the AC-3 control:</p> <ul style="list-style-type: none"> - FDP_IFC.1 (User Data Protection/ Information Flow Control Policy/ Subset Information Flow Control); and - FDP_IFF.4 (User Data Protection/ Information Flow Control Functions/ Simple Security Attributes).
<p>AC-3 (7) Access Control / Access Enforcement / Role-Based Access Control</p> <p>Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].</p> <p>Supplemental Guidance:</p> <p>Role-based access control (RBAC) is an access control policy that restricts system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.</p> <p>Related Controls: PE-2</p>	<p>800-171 CUI</p>	<p>P</p> <p>The following Trend Micro products use RBAC to enforce access control.</p> <p>Deep Discovery Inspector restricts access to authorized product administrators' using role-based access control. All product administrators are assigned roles at creation. Authorized product administrators can only access the product through the administrative interface. They have full access to the functions permitted by their roles.</p> <p>Deep Discovery Email Inspector uses Role-Based Access Control to grant and control access to the privileged management console. This feature is used to assign specific management console privileges to accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users log on to the management console using custom user accounts.</p> <p>Deep Discovery Analyzer makes use of Role Based Access Control for administration, the Role-based administration streamlines how administrators configure user accounts and control access to the management console.</p> <p>Deep Security access control includes Role-based access which allows multiple administrators, each with different sets of access and editing rights, to edit and monitor different aspects of the system and receive information appropriate to them. In addition, digital signatures are used to authenticate system components and verify the integrity of rules.</p> <p>TippingPoint SMS allows the creation of roles and full customization of privileges assigned to each role. The use of Role Based Access Controls using the username, which is used to identify the role of the user and the password to authenticate them. There are three roles (Operator, Administrator, Super-user) that can be assigned to a user. SMS also allows the creation of customer roles and full customization of privileges assigned to each role.</p> <p>-----</p> <p>Evidence of these capability are further addressed in the Deep Discovery Inspector, Deep Security and TippingPoint Common Criteria, Security Target requirement class FMT: Security Management and specifically FMT_SMR.1 Security Roles, The TippingPoint Security Functions maintain the roles Super-user, Administrator, Operator.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
			<p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AC-3 (7) control:</p> <ul style="list-style-type: none"> - FMT_MOF.1 (<i>Security Management/ Management of Functions in TSE</i>); - FMT_MTD.1 (<i>Security Management/ Management of TSF Data</i>); and - FMT_SMR.1 (<i>Security Management/ Security Management Roles/ Security Roles</i>).
AC-4 Access Control / Information Flow Enforcement			
<p>AC-4 Access Control / Information Flow Enforcement</p> <p>Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].</p> <p>Supplemental Guidance:</p> <p>Information flow control regulates where information can travel within a system and between systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between systems in different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example, prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.</p> <p>Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet filtering capability based on header information, or message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related Controls: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-9, CM-7, PM-25, SC-4, SC-7, SC-16, SC-31.</p> <p>References: NIST Special Publications 800-162, 800-178.</p>	<p>M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p>	<p>Deep Security firewall capabilities limit communication between various endpoints. The Intrusion Prevention module inspects incoming and outgoing traffic to detect and block suspicious activity. This prevents exploitation of known and zero-day vulnerabilities. IPS module has the capability to prevent specific applications (ie. BitTorrent) from entering the system.</p> <p>TippingPoint: The main component of the TippingPoint IPS device is the Threat Suppression Engine (TSE), a custom engine that detects and blocks a broad range of attacks at wire speeds. The TSE is a flow-based network security engine, in which each packet is identified as a component of a flow and each flow is tracked in the connection table on the IPS. A flow is uniquely identified by its packet header information:</p> <ul style="list-style-type: none"> - IPv4 or IPv6 protocol (ICMP, TCP, UDP, other) - source and destination IP addresses - source and destination ports <p>The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. When a packet matches an IPS filter, the IPS handles the packets based on the action set configured on the filter. For example, if the action set is Block, then the packet is dropped and subsequent packets from the same flow are dropped without inspection. The IPS device provides default actions to block or permit traffic with options to quarantine or rate-limit traffic and to notify users or systems when an action executes.</p> <p>In addition TippingPoint addresses this requirement for Information Flow Enforcement and evidence of this is provided in the TippingPoint Common Criteria Security Target EAL3 User Data Protection, Subset Information Flow Control (FDP_IFC.1) and Simple Security Attributes (FDP_IFF.1).</p> <p>FDP_IFC.1 -- TippingPoint enforces flow control of information on:</p> <ul style="list-style-type: none"> - Subjects: unauthenticated external IT entities that send and receive information through TippingPoint; - Information: traffic sent through TippingPoint from one subject to another; and - Operations: pass information. <p>FDP_IFF.1 -- TippingPoint enforces the flow control based on the following types of subject and information security attributes:</p> <ul style="list-style-type: none"> - Subject security attributes: presumed IP address; - Information security attributes: protocol, source IP address, source port, destination IP address, destination port. <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>“provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.”</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AC-4 control:</p> <ul style="list-style-type: none"> - FDP_IFC.1 (<i>User Data Protection/ Information Flow Control Policy/ Information Flow Control</i>); and - FDP_IFF.1 (<i>User Data Protection/ Information Flow Control Functions/ Simple Security Attributes</i>).

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>AC-4 (1) Access Control / Information Flow Enforcement / Object Security Attributes</p> <p>Use [Assignment: organization-defined security attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.</p> <p>Supplemental Guidance:</p> <p>Information flow enforcement mechanisms compare security attributes associated with information (data content and data structure) and source/destination objects, and respond appropriately when the mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled Secret would be allowed to flow to a destination object labeled Secret, but an information object labeled Top Secret would not be allowed to flow to a destination object labeled Secret. Security attributes can also include, for example, source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information.</p>		E P	<p>Deep Security has the capability to assign firewall rules to a policy used by computers that trusted traffic flows through.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AC-4 (1) control:</p> <ul style="list-style-type: none"> - FDP_IFC.1 (<i>User Data Protection/ Information Flow Control Policy/ Information Flow Control</i>); and - FDP_IFF.1 (<i>User Data Protection/ Information Flow Control Functions/ Simple Security Attributes</i>).
<p>AC-4 (2) Access Control / Information Flow Enforcement / Processing Domains</p> <p>Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.</p> <p>Supplemental Guidance:</p> <p>Within systems, protected processing domains are processing spaces that have controlled interactions with other processing spaces, enabling control of information flows between these spaces and to/from data/information objects. A protected processing domain can be provided, for example, by implementing domain and type enforcement. In domain and type enforcement, system processes are assigned to domains; information is identified by types; and information flows are controlled based on allowed information accesses (determined by domain and type), allowed signaling among domains, and allowed process transitions to other domains.</p> <p>Related Controls: SC-39.</p>		P	<p>TippingPoint addresses this requirement for Information Flow Enforcement Processing Domains and evidence of this is provided in the TippingPoint Common Criteria Security Target EAL3 User Data Protection, Simple Security Attributes (FDP_IFF.1). TippingPoint enforces the flow control based on the following types of subject and information security attributes:</p> <ul style="list-style-type: none"> • Subject security attributes: presumed IP address; • Information security attributes: protocol, source IP address, source port, destination IP address, destination port <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AC-4 (2) control:</p> <ul style="list-style-type: none"> - FDP_IFF.1 (<i>User Data Protection/ Information Flow Control Functions/ Simple Security Attributes</i>).
<p>AC-4 (4) Access Control / Information Flow Enforcement / Content Check Encrypted Information</p> <p>Prevent encrypted information from bypassing [Assignment: organization-defined flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].</p> <p>Supplemental Guidance:</p> <p>Content checking, security policy filters, and data type identifiers are examples of flow control mechanisms.</p> <p>Related Controls: SI-4.</p>	H 800-171 CUI	E	<p>Deep Discovery Inspector Use is made of 3rd party solutions to decrypt SSL traffic. SSL decryption policies are implemented which for example allow encrypted access to finance and shopping categories, but decrypt and inspect traffic to all other URL categories.</p> <p>Deep Discovery Email Inspector Use is made of 3rd party solutions to decrypt SSL traffic. SSL decryption policies are implemented which allow for example encrypted access to finance and shopping categories, but decrypt and inspect traffic to all other URL categories. Deep Discovery Email Inspector supports the ability for encrypted document password guessing or email password extraction.</p> <p>Deep Security allows packet data capture on encrypted traffic (SSL or TLS): To provide the capability to inspect SSL or TLS traffic - the intrusion prevention module, can be configured for SSL or TLS inspection for a given credential-port pair on one or more interfaces of a protected computer. The Intrusion Prevention module allows the recording of the packet data that triggers Intrusion Prevention Rules. This setting turns on data capture when Intrusion Prevention rules are being applied to encrypted traffic.</p>

AC-5 Access Control / Separation of Duties

<p>AC-5 Access Control / Separation of Duties</p> <ul style="list-style-type: none"> a. Separate [Assignment: organization-defined duties of individuals]; b. Document separation of duties of individuals; and c. Define system access authorizations to support separation of duties. <p>Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example, dividing mission functions and system support functions among different individuals and/or roles; conducting system support functions with different individuals; and ensuring security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.</p> <p>Related Controls: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-5, MA-3, MA-5, PS-2, SA-17.</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector can only be accessed by authorized system administrator and authorized administrators. This capability assists with separation of duties by providing specific roles and access controls. The Version 3.2 of the product is certified by the Common Criteria Evaluation and Certification Scheme (CCS) to the EAL2+ level carried out by the Communications Security Establishment Canada which provides evidence of this capability.</p> <p>Deep Discovery Email Inspector delegates tasks to different security and network administrators to provide separation of duties in Deep Discovery Email Inspector administration.</p> <ul style="list-style-type: none"> - Administrator Users have complete access to the features and settings contained in the menu items: Dashboard; Detections; Policy; Alerts/Reports; Logs; Administration; and Help. - Investigator Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications: Dashboard; Detections; Alerts/Reports > Reports > Generated Reports; Alerts/Reports > Alerts > Triggered Alerts; Logs; and Help. - Operator Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications: Dashboard; Detections (no access to message body); Alerts/Reports > Reports > Generated Reports; Alerts/Reports > Alerts > Triggered Alerts; Logs; and Help. <p>Deep Discovery Analyzer: The separation of duties is accomplished using different roles:</p> <ul style="list-style-type: none"> - Administrators have full access to submitted objects, analysis results, and product settings - Investigators have read-only access to submitted objects, analysis results, and product settings, but can submit objects and download the investigation package, including submitted objects - Operators have read-only access to submitted objects, analysis results, and product settings <p>Deep Security: Assists separation of duties by providing specific roles and access controls. The product has been evaluated and certified to the EAL2 level, to provide evidence of this capability.</p> <p>TippingPoint - The SMS provides this functionality which allows custom Groups and Roles to be created. The role creation allows for granular permissions assignments. The TippingPoint solution provides separation of duties through one of three access levels for each user account:</p> <ul style="list-style-type: none"> - Operator — Base-level administrator user who monitors the system and network traffic. - Administrator — Enhanced administrator user who can view, manage, and configure functions and options in the system. - Super user — Administrator user who has full access to all Local Security Managers and Command Line Interface functions. <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AC-5 control:</p> <ul style="list-style-type: none"> - FMT_SMR.1 (Security Management/ Security Management Roles/ Security Roles).
--	--	----------	--

AC-6 Access Control / Least Privilege

<p>AC-6 Access Control / Least Privilege</p> <p>Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.</p> <p>Supplemental Guidance: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems.</p> <p>Related Controls: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-15, SA-17, SC-38.</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector: Can only be accessed by authorized system administrator and authorized administrators. This capability assists with Least Privilege by providing specific roles and access controls. The product is certified by the Common Criteria Evaluation and Certification Scheme (CCS) to the EAL2+ level carried out by the Communications Security Establishment Canada which provides evidence of this capability.</p> <p>Deep Discovery Email Inspector: Delegates tasks to different security and network administrators to provide Least Privilege in Deep Discovery Email Inspector administration.</p> <ul style="list-style-type: none"> - Administrator users have complete access to the features and settings contained in the menu items: Dashboard; Detections; Policy; Alerts/Reports; Logs; Administration; and Help. - Investigator users can view certain features and settings contained in the menu items, but cannot make any administrative modifications: Dashboard; Detections; Alerts/Reports > Reports > Generated Reports; Alerts/Reports > Alerts > Triggered Alerts; Logs; and Help. - Operator users can view certain features and settings contained in the menu items, but cannot make any administrative modifications: Dashboard; Detections (no access to message body); Alerts/Reports > Reports > Generated Reports; Alerts / Reports > Alerts > Triggered Alerts; Logs; and Help. <p>Deep Discovery Analyzer: The Least Privilege is accomplished using different roles:</p> <ul style="list-style-type: none"> - Administrators have full access to submitted objects, analysis results, and product settings - Investigators have read-only access to submitted objects, analysis results, and product settings, but can submit objects and download the investigation package, including submitted objects - Operators have read-only access to submitted objects, analysis results, and product settings <p>Deep Security: Assists in Least Privilege by providing specific roles and access controls. The product has been evaluated and certified to the EAL2 level, to provide evidence of this capability.</p> <p>TippingPoint - The TippingPoint solution provides Least Privilege through one of three access levels for each user account:</p> <ul style="list-style-type: none"> - Operator — Base-level administrator user who monitors the system and network traffic. - Administrator — Enhanced administrator user who can view, manage, and configure functions and options in the system. - Super user — Administrator user who has full access to all Local Security Managers and Command Line Interface functions <p>The TippingPoint SMS provides custom Groups and Roles to be created which are associated with the levels of privilege.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AC-6 control:</p> <ul style="list-style-type: none"> - FMT_MOF.1 (Security Management/ Security Management Roles/ Security Roles); - FMT_MTD.1 (Security Management/ Management of TSF Data); and - FMT_SMR.1 (Security Management/ Security Management Roles/ Security Roles).
--	--	----------	--

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>AC-6 (1) Access Control / Least Privilege / Authorize Access to Security Functions</p> <p>Explicitly authorize access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].</p> <p>Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and establishing intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.</p> <p>Related Controls: AC-17, AC-18, AC-19, AU-9, PE-2.</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector assists with this requirement by explicitly authorizing access to security functions through roles with specific permissions and privileges, and defining audit events. Deep Discovery Inspector provides control of access to selected sections of the management console. Deep Discovery Inspector supports 128 local accounts and 512 Active Directory accounts or groups, including the following roles:</p> <ul style="list-style-type: none"> - System administrator (default) - Administrator (user-created) - Viewer (user-created) <p>All users (system administrator, other administrators, viewers) share one dashboard. Each management console viewer account is provided a partially independent dashboard. Changes to any account's dashboard affect the dashboards of other accounts.</p> <p>Deep Discovery Email Inspector delegates tasks to different security and network administrators to provide authorized access to security functions</p> <ul style="list-style-type: none"> - Administrator users have complete access to the features and settings contained in the menu items: Dashboard; Detections; Policy; Alerts/Reports; Logs; and Administration. - Investigator users can view certain features and settings contained in the menu items, but cannot make any administrative modifications: Dashboard; Detections; Alerts/Reports > Reports > Generated Reports; Alerts/Reports > Alerts > Triggered Alerts; and Logs. - Operator users can view certain features and settings contained in the menu items, but cannot make any administrative modifications: Dashboard; Detections (no access to message body); Alerts/Reports > Reports > Generated Reports; Alerts/Reports > Alerts > Triggered Alerts; and Logs. <p>Deep Discovery Analyzer authorized access to security functions is accomplished using different roles:</p> <ul style="list-style-type: none"> - Administrators have full access to submitted objects, analysis results, and product settings. - Investigators have read-only access to submitted objects, analysis results, and product settings, but can submit objects and download the investigation package, including submitted objects - Operators have read-only access to submitted objects, analysis results, and product settings <p>Deep Security comes preconfigured with two roles:</p> <ul style="list-style-type: none"> - Full Access: The full access role grants the user all possible privileges in terms of managing the Deep Security system including creating, editing, and deleting computers, computer groups, policies, rules, malware scan configurations, and others. - Auditor: The auditor role gives the user the ability to view all the information in the Deep Security system but without the ability to make any modifications except to their own personal settings, such as password, contact information, dashboard layout preferences, and others. <p>It should be noted that on initial installation the first user is the Master Administrator and that user has full access. The Master Administrator can then create all subsequent roles and users.</p> <p>TippingPoint The SMS provides this functionality once the IPS is managed by an SMS, all operations local to the IPS are read only and the SMS controls everything. The Local Security Manager (LSM) authentication enables administrators to create and manage user accounts, set user account preferences, and manage X.509 certificates. A user account provides users with access to the TippingPoint Operating System (TOS) to manage IPS devices through the LSM web interface or from the Command Line Interface (CLI). The management functions available to a user are determined by the account security level configured on the account. Accounts can only be defined in the embedded TOS user database on the IPS.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
			<p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AC-6 (1) control:</p> <ul style="list-style-type: none"> - FMT_MOF.1 (<i>Security Management/ Management of Functions in TSF</i>); and - FMT_MTD.1 (<i>Security Management/ Management of TSF Data</i>).
<p>AC-6 (2) Least Privilege / Non-Privileged Access for Nonsecurity Functions Require that users of system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.</p> <p>Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.</p> <p>Related Controls: AC-17, AC-18, AC-19, PL-4.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector assists with this requirement by permitting access to non security functions through non-privileged accounts, through role based access control for such roles as Viewer. Deep Discovery Inspector provides control of access to selected sections of the management console. Deep Discovery Inspector supports 128 local accounts and 512 Active Directory accounts or groups, including the following roles:</p> <ul style="list-style-type: none"> - System administrator (default) - Administrator (user-created) - Viewer (user-created) <p>Deep Discovery Email Inspector: Delegates tasks to different administrators to provide non privileged access to non-security functions. Operator users can view certain features and settings contained in the menu items, but cannot make any administrative modifications.</p> <p>Deep Discovery Analyzer: non-privileged access to non security functions is accomplished using roles such as Operators have read-only access to submitted objects, analysis results, and product settings</p> <p>Deep Security permits non privileged users access to non security function through role based access control. Roles can be created that can restrict users from editing or even seeing Deep Security objects such as specific computers, the properties of security rules, or the system settings.</p> <p>TippingPoint the SMS provides this functionality in a granular way. It allows custom Groups and Roles to be created. The role creation allows for granular permissions assignments to assist with the non privileged access to non security functions through the different access levels for each user account, such as the Operator — Base-level user who can only monitors the system and network traffic.</p>
<p>AC-6 (4) Access Control / Least Privilege / Separate Processing Domains Provide separate processing domains to enable finer-grained allocation of user privileges.</p> <p>Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example, using virtualization techniques to allow additional user privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; employing hardware/software domain separation mechanisms; and implementing separate physical domains.</p> <p>Related Controls: AC-4, SC-2, SC-3, SC-30, SC-32, SC-39.</p>	800-171 CUI	E	<p>Deep Security assists in meeting this requirement by providing machine or domain separation through the implementation of firewall rules/filters on specific virtual machines or physical machines to create separate processing domains/zones. This allows additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine. Deep Security within a virtualized environment provides agentless security at the hypervisor level. This security provided by the Deep Security Virtual Appliance. The virtual appliance is deployed at the cluster level through NSX Manager to offer protection to VMs on a given host. Through integration with VMware NSX Advanced or Enterprise, the Deep Security Virtual Appliance can perform firewall, intrusion prevention, anti-malware (Windows only) and file integrity monitoring capabilities (Windows only) for all protected VMs</p> <p>TippingPoint performs this function through Virtual Segments. This allows for separate policy processing "domains" and enables finer-grained allocation of privileges in regards to network traffic..</p>
<p>AC-6 (10) Access Control / Least Privilege / Prohibit Non-Privileged Users From Executing Privileged Functions The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.</p> <p>Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector provides a self-protection capability which is addressed by the Common Criteria evaluations of Deep Discovery Inspector certified by the Common Criteria Evaluation and Certification Scheme (CCS) carried out by the Communications Security Establishment Canada. Deep Discovery Inspector addresses a non privileged user from executing privileged functions as detailed in the Common Criteria Deep Discovery Inspector Architectural Design which provides a description of the security architecture and provides details of the security functional requirements enforcing design. It describes the security domains maintained by the Deep Discovery Inspector security functions, how the initialization process is secure, how the Deep Discovery Inspector security function protect itself from tampering and prevents bypass of the security functional requirements enforcing functionality.</p> <p>Deep Security Common Criteria Security Target provides the evidence that Deep Security protects the security functions through:</p> <ul style="list-style-type: none"> - Basic internal Deep Security, Security Function data transfer protection (FPT_ITT.1) Deep Security, security functions protect Deep Security security function data from disclosure and modification when it is transmitted between separate parts of Deep Security.

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>C-6 (10) Access Control / Least Privilege / Prohibit Non-Privileged Users From Executing Privileged Functions</p> <p>(... Continued.)</p>		<ul style="list-style-type: none"> - Guarantee of System Data Availability (IDS_STG.1, EXT) Deep Security protects the stored System data from unauthorized deletion. (EXT) IDS_STG.1.1 - Deep Security protects the stored System data from modification. (EXT) IDS_STG.1.2 - Deep Security ensures that the most recent System data will be maintained when the following conditions occur: System data storage exhaustion. (EXT) IDS_STG.1.3 <p>TippingPoint The TippingPoint SMS provides this type of functionality in a granular way through the creation of custom Groups and Roles. The role creation allows for granular permissions assignments. In addition TippingPoint addresses a non-privileged user from executing privileged functions by:</p> <ul style="list-style-type: none"> - Users are identified and authenticated before gaining access to the capabilities of TippingPoint - Users are restricted in how they can access the management capabilities of TippingPoint, based on their assigned authorization level. - The operational environment provides capabilities to protect the confidentiality of data communicated by administrative users (including authentication data) to TippingPoint <p>In addition TippingPoint provides Guarantee of IDS Data Availability (IDS_STG_EXT.1)</p> <ul style="list-style-type: none"> - Protects the stored IDS data from unauthorized deletion. - Protects the stored IDS data from modification. - Ensures that [the most recent 50% of the] IDS data will be maintained when IDS data storage exhaustion occurs.
AC-7 Access Control / Unsuccessful Logon Attempts		
<p>AC-7 Access Control / Unsuccessful Logon Attempts</p> <p>a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time-period]; and</p> <p>b. Automatically [Selection (one or more): lock the account/node for an [Assignment: organization-defined time-period]; lock the account/node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; take [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.</p> <p>Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined time established by organizations. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.</p> <p>Related Controls: AC-2, AC-9, AU-2, AU-6, IA-5.</p> <p>References: NIST Special Publications 800-63, 800-124.</p>	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p> <p>Deep Discovery Analyzer includes a security feature that locks an account in case the user typed an incorrect password five times in a row. This feature cannot be disabled. Accounts locked this way, including administrator accounts, unlock automatically after ten minutes. The administrator can manually unlock accounts that have been locked. Only one user account can be unlocked at a time</p> <p>Deep Security makes use of integrity monitoring rules to provide indicators of compromise for password related controls of the enterprise. The UserSet element represents a set of users which can be used to control the following password related attributes:</p> <ul style="list-style-type: none"> - cannotChangePassword: True or false indicating if the user is permitted to change their password. - disabled: True or false indicating if the account has been disabled. On Windows systems this reflects the "disabled" checkbox for the user. On Unix systems this will be true if the user's account has expired or if their password has expired and they've exceeded the inactivity grace period for changing it. - lockedOut: True or false indicating if the user has been locked out, either explicitly or due to excessive failed password attempts. - passwordHasExpired: True or false indicating if the user's password has expired. Note that on Windows this attribute is only available on Windows XP and newer operating systems. (Not available in AIX) - passwordLastChanged: The timestamp of the last time the user's password was changed. This is recorded by the DSA as the number of milliseconds since Jan 1 1970 UTC - Deep Security Manager renders the timestamp in local time based on this value. Note that on Unix platforms the resolution of this attribute is one day, so the time component of the rendered timestamp is meaningless. (N/A in AIX) - passwordNeverExpires: True or false indicating if the password does not expire. <p>The Deep Security integrity monitoring capability can also use a composite rule that for example creates a higher severity alert after five failed passwords within a period of 10 minutes. Using the <code><if_matched_sid></if_matched_sid></code> tag indicates which rule needs to be seen within the desired frequency and timeframe for the new rule to create an alert.</p> <p>TippingPoint addresses Authentication Failure Handling as indicated in the Common Criteria Security Target by:</p> <ul style="list-style-type: none"> - FIA_AFL.1.1 – TippingPoint detects when an administrator configurable positive integer within [1..10] unsuccessful authentication attempts occur related to user login. - FIA_AFL.1.2 – When the defined number of unsuccessful authentication attempts has been met, TippingPoint performs the configured Failed Login Action, which can be one of the following:

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
AC-7 Access Control / Unsuccessful Logon Attempts (... Continued.)			<ul style="list-style-type: none"> - Lock the account for a configured Lockout Period; - Disable the account; - Generate an audit event documenting the failed login attempt]. <p>----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AC-7 control:</p> <ul style="list-style-type: none"> - FIA_AFL.1 (Identification and Authentication/ Authentication Failures/ Authentication Failure Handling)
AC-7 (3) Access Control / Unsuccessful Logon Attempts / Biometric Attempt Limiting Limit the number of unsuccessful biometric logon attempts to [Assignment: organization-defined number]. Supplemental Guidance: Biometrics are probabilistic in nature. The ability to successfully authenticate can be impacted by many factors, including matching performance and presentation attack detection mechanisms. Organizations select the appropriate number of attempts and fall back mechanisms for users based on these, and other organizationally defined factors. Related Controls: IA-3.	800-171 CUI	E	<p>Deep Security using Log Inspection rules can assist in meeting this control by analyzing log files and detecting Unsuccessful Logon Attempts. Use is made of the OSSEC log inspection engine which is integrated into Deep Security Agents and gives Deep Security the ability to inspect the logs and events generated by the operating system and applications running on the computer. Log Inspection can forward suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving.</p>
AC-14 Access Control / Permitted Actions without Identification or Authorization			
AC-14 Access Control / Permitted Actions without Identification or Authorization a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational missions and business functions; and b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication. Supplemental Guidance: This control addresses situations in which organizations determine that no identification or authentication is required in organizational systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication and therefore, the values for assignment statements can be none. Related Controls: AC-8, IA-2, PL-2.	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector provides evidence of supporting this control through the Common Criteria Security Target, specifically the Timing of Authentication (FIA_UAU.1). Deep Discovery Inspector shall allow no action on behalf of the user to be performed before the user is authenticated.</p> <p>Deep Security allows limited actions on behalf of the user to be performed before the user is identified. FIA_UID.1. The URLs accessible without Authentication are as shown in the Security Target and include: The Authentication Page; The Error Screen; The welcome page that redirects to SignIn.screen; The 404 page not found screen; The 413 page upload too big; and other similar pages.</p> <p>TippingPoint as shown in the Common Criteria Security Target, requires each user to be successfully authenticated before allowing any other security function actions on behalf of that user. Also requires each user to be successfully identified before allowing any other security function mediated actions on behalf of that user.</p> <p>----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security and Deep Discovery Inspector CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AC-14 control:</p> <ul style="list-style-type: none"> - FIA_UAU.1 (Identification and Authentication/ User Authentication/ Timing of Authentication); and - FIA_UID.1 (Identification and Authentication/ User Identification/ Timing of Identification). <p>The TippingPoint CC Security Target includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AC-14 control:</p> <ul style="list-style-type: none"> - FIA_UAU.2 (Identification and Authentication/ User Authentication/ User Action before any Action); and - FIA_UID.2 (Identification and Authentication/ User Identification/ User Identification Before any Action).

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
AC-16 Access Control / Security and Privacy Attributes		
<p>AC-16 Access Control / Security and Privacy Attributes</p> <p>a. Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] having [Assignment: organization-defined security and privacy attribute values] with information in storage, in process, and/or in transmission;</p> <p>b. Ensure that the security and privacy attribute associations are made and retained with the information;</p> <p>c. Establish the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined systems]; and</p> <p>d. Determine the permitted [Assignment: organization-defined values or ranges] for each of the established security and privacy attributes.</p> <p>Supplemental Guidance:</p> <p>Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, interprocess pipes, and communications ports. Security attributes, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. Privacy attributes, which may be used independently, or in conjunction with security attributes, represent the basic properties or characteristics of an entity with respect to the management of personally identifiable information. Such attributes are used to enable the implementation of the need for the record in the performance of duties, the identification of personal information within data objects, and the identification of permitted uses of personal information. Attributes can be explicitly or implicitly associated with the information contained in organizational systems or system components.</p> <p>Security and privacy attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects, or to change the system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security and privacy attributes to subjects and objects is referred to as binding and is inclusive of setting the attribute value and the attribute type. Security and privacy attributes when bound to data or information, enable the enforcement of security policies for access control and information flow control and privacy policies including, for example, for data retention limits and permitted uses of personally identifiable information. Such enforcement occurs through organizational processes or system functions or mechanisms. Binding techniques implemented by systems affect the strength of attribute binding to information. Binding strength and the assurance associated with binding techniques play an important part in the trust organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. The content or assigned values of the security and privacy attributes can directly affect the ability of individuals to access organizational information.</p> <p>Organizations can define the types of attributes needed for selected systems to support missions or business functions. There is potentially a wide range of values that can be assigned to any given security attribute. Release markings can include, for example, US only, NATO, or NOFORN (not releasable to foreign nationals). By specifying permitted attribute ranges and values, organizations ensure that the security and privacy attribute values are meaningful and relevant. Labeling refers to the association of security and privacy attributes with subjects and objects represented by the internal data structures within organizational systems. This facilitates system-based enforcement of information security and privacy policies. Labels include, for example, access authorizations, nationality, data life cycle protection (i.e., encryption and data expiration), data subject consents, permissible data uses, affiliation as contractor, and classification of information in accordance with legal and compliance requirements. Conversely, marking refers to the association of security and privacy attributes with objects in a human-readable form. This enables manual, procedural, or process-based enforcement of information security and privacy policies. Examples of attribute types include classification level for objects and clearance (access authorization) level for subjects. An attribute value for both attribute types is Top Secret. Related Controls: AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, IP-2, MP-3, PE-22, SC-11, SC-16, SI-12. References: FIPS Publications 140-2, 186-4; NIST Special Publications 800-162, 800-178.</p>	<p>CNSSI</p>	<p>E P</p> <p>Deep Discovery Inspector operates out of band and is capable of detecting network anomalies using a combination of network centric rules and file based sandboxing.</p> <p>Deep Discovery Email Inspector operates in-line or out of band and is capable of detecting email based anomalies using a combination of network centric rules and file based sandboxing.</p> <p>Deep Security Firewall uses fine-grained filtering these rules filter traffic based on source and destination IP address, port, MAC address, etc. Different rules can be applied to different network interfaces. For end-user systems, the firewall is location aware, and is able to limit interface use such that only a single interface can be used at one time.</p> <p>Deep Security Integrity Monitoring file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.) and Security Policies allow Integrity Monitoring rules to be configured for groups of systems, or individual systems.</p> <p>TippingPoint addresses this requirement through the Threat Suppression Engine component which provides traffic management filters that can be applied to traffic on selected segments, allowing TippingPoint to enforce an information flow control policy and operate as a firewall. Traffic management filters are managed within the context of a Traffic Management Profile that identifies the segment to which the Profile applies.</p> <p>TippingPoint provides evidence of this through the Common Criteria, Security Function, Simple Security Attributes (FDP_IFF.1) by enforcing the [Traffic Management SFP] based on the following types of subject and information security attributes:</p> <ul style="list-style-type: none"> - Subject security attributes: presumed IP address - Information security attributes: protocol, source IP address, source port, destination IP address, destination port. <p>The main component of the IPS device is the Threat Suppression Engine (TSE), a custom engine that detects and blocks a broad range of attacks at wire speeds. The TSE is a flow-based network security engine, in which each packet is identified as a component of a flow and each flow is tracked in the connection table on the IPS. A flow is uniquely identified by its packet header information:</p> <ul style="list-style-type: none"> - IPv4 or IPv6 protocol (ICMP, TCP, UDP, other) - source and destination IP addresses - source and destination ports <p>The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. When a packet matches an IPS filter, the IPS handles the packets based on the action set configured on the filter. For example, if the action set is Block, then the packet is dropped and subsequent packets from the same flow are dropped without inspection. The IPS device provides default actions to block or permit traffic with options to quarantine or rate-limit traffic and to notify users or systems when an action executes.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AC-16 control:</p> <ul style="list-style-type: none"> - FDP_IFF.1 (<i>User Data Protection/ Information Flow Control Functions/ Simple Security Attributes</i>)

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy	
AC-16 (11) Access Control / Security and Privacy Attributes / Audit Changes Audit changes to security and privacy attributes.	800-171 CUI	E	Deep Security provides auditable reporting along with alert generations, and automated report creation and delivery. The Deep Security Log Inspection provides: <ul style="list-style-type: none">- Suspicious behavior detection.- Collecting events across heterogeneous environments containing different operating systems and diverse applications.- Insight and knowledge of important events such as error and informational events (disk full, service start/shutdown, etc.).		
AC-17 Access Control / Remote Access					
AC-17 (2) Access Control / Remote Access / Protection of Confidentiality / Integrity Using Encryption Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related Controls: SC-8, SC-12, SC-13.	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	Deep Discovery Inspector supports compliance with this requirement through the use of the TLS/SSL protocol for remote access. Deep Discovery Email Inspector supports compliance with this requirement by Endpoints connecting to Deep Discovery Email Inspector through SSH. Deep Discovery Analyzer is a secure environment that manages and analyzes objects submitted by integrated products, and administrators and investigators (through SSH) Deep Security supports compliance with this requirement through the use of the TLS/SSL protocol for remote access. TippingPoint management clients, connect via the network management port, to support remote management. The management client in turn requires an SSHv2 client to connect to the CLI. TippingPoint also provides a trusted path for remote administrative users. The trusted path is implemented over the network management port using HTTPS for access to the LSM and SSHv2 for access to the CLI. Remote users initiate the trusted path by establishing an HTTPS connection (using a supported web browser) or SSH session (using an SSH client). The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS or SSHv2 ensures all communication over the trusted path is protected from disclosure and undetected modification.		
AC-18 Access Control / Wireless Access					
AC-18 (4) Access Control / Wireless Access / Restrict Configurations by Users Identify and explicitly authorize users allowed to independently configure wireless networking capabilities. Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational systems. Related Controls: SC-7, SC-15.	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	Deep Security can assist in meeting this requirement to control wireless configuration by the use of Deep Security Firewall rules for wireless laptops. Deep Security addresses the problem where many laptops are capable of connecting to both the wired and wireless networks, organizations need to be aware of the problems that can result from this scenario. The common problem is a "network bridge" configured between the wired and wireless network. There is a risk of forwarding the internal traffic externally and potentially expose internal hosts to external attacks. Deep Security allows administrators to configure a set of firewall rules for these types of users to prevent them from creating a network bridge. Deep Security can assign various elements of a policy (firewall rules, etc.) to each wireless interface and to apply special rules only to the wireless network interface, interface types can be used to accomplish this.		
AC-25 Access Control / Reference Monitor					
AC-25 Access Control / Reference Monitor Implement a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured. Supplemental Guidance: Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Reference monitors enforce mandatory access control policies, a type of access control that restricts access to objects based on the identity of subjects or groups to which the subjects belong. The access controls are mandatory because subjects with certain privileges (i.e., access permissions) are restricted from passing those privileges on to any other subjects, either directly or indirectly - that is, the system strictly enforces the access control policy based on the rule	800-171 CUI	P	CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls. The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AC-25 control: <ul style="list-style-type: none">- ADV_ARC.1 (<i>Development/ Security Architecture Description</i>): ADV_ARC.1.1D "... security features of the TSF cannot be bypassed".		

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>set established by the policy. The tamperproof property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The always invoked property prevents adversaries from bypassing the mechanism and hence violating the security policy. The smallness property helps to ensure the completeness in the analysis and testing of the mechanism to detect weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy.</p> <p>Related Controls: AC-3, AC-16, SC-3, SC-11, SC-39, SI-13.</p>		
AU-2 Audit and Accountability / Auditable Events		
<p>AU-2 Audit Events</p> <p>a. Verify that the system can audit the following event types: [Assignment: organization-defined auditable event types];</p> <p>b. Coordinate the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable event types;</p> <p>c. Provide a rationale for why the auditable event types are deemed to be adequate to support after-the-fact investigations of security and privacy incidents; and</p> <p>d. Specify that the following event types are to be audited within the system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].</p> <p>Supplemental Guidance:</p> <p>An event is any observable occurrence in an organizational system. Organizations identify audit event types as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing audit needs. Audit event types can include, for example, password changes; failed logons or failed accesses related to systems; security attribute changes, administrative privilege usage, PIV credential usage, query parameters, or external credential usage. In determining the set of auditable event types, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other system needs, this control also requires identifying that subset of auditable event types that are audited at a given point in time. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.</p> <p>Auditing requirements, including the need for auditable events, may be referenced in other security and privacy controls and control enhancements for example, AC-2(4), AC-3(10), AC6(9), AC-16(11), AC-17(1), CM-3.f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PA-4.d, PE-3, PM22, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations also include auditable event types that are required by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network.</p> <p>Selecting the appropriate level of auditing is an important aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable event types, the auditing necessary to cover related event types such as the steps in distributed, transaction-based processes and actions that occur in service-oriented architectures. Related Controls: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU7, AU-11, AU-12, CM-3, CM-5, CM-6, IA-3, MA-4, MP-4, PA-4, PE-3, PM-22, RA-8, SC-7, SC18, SI-3, SI-4, SI-7, SI-10, SI-11.</p> <p>References: NIST Special Publication 800-92.</p>	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p> <p>E P</p>	<p>Deep Discovery Inspector (DDI) supports compliance with AU-2 and AU-3 requirements by enabling organizations to audit and log security related events through inspection of network traffic between and within an organization's network including: communications or links to suspicious/malicious endpoints, suspicious/malicious network traffic, and infected files. Logs include, time stamps, source and destination addresses, identifiers, event descriptions, success/fail indications, rules involved. Security event information can be integrated with an organization's syslog server or SIEM product. Audit events include:</p> <ul style="list-style-type: none"> Start-up and shutdown of audit functions; Access to system; Access to Deep Discovery Inspector and system data - Object IDs, requested access; Reading of information from the audit records; Unsuccessful attempts to read information from the audit records; All modifications to the audit configuration that occur while the audit collection functions are operating; All use of the authentication mechanism - User identity, location; All use of the user identification mechanism -User identity, location; All modifications in the behavior of the functions of the Deep Discovery Inspector security functions; All modifications to the values of Deep Discovery Inspector security function data; and Modifications to the group of users that are part of a role - User identity. <p>DDI audit functionality includes:</p> <ul style="list-style-type: none"> <u>Audit Review</u> - Authorized system administrators can read all audit information in a manner suitable to interpret the information; <u>Restricted Audit Review</u> - Prohibits all users read access to the audit records, except those that have been granted explicit read-access; Authorized system administrator functions include: <ul style="list-style-type: none"> <u>Selectable Audit Review</u> - ability to review and sort audit data based on date and time, subject identity, type of event, and success or failure of related event; <u>Selective Audit</u> - include or exclude auditable events from the set of audited events based on event type. <u>Guarantees of Audit Data Availability</u> - Protects the stored audit records from unauthorized deletion. Prevents modifications to the audit records, and ensure that the latest recorded audit records will be maintained when audit storage is exhausted. <u>Prevention of Audit Data Loss</u> - Overwrites the oldest stored audit records and sends an alarm if the audit trail is full. <p>Deep Discovery Email Inspector (DDEI) supports compliance with the AU-2 and AU-3 requirements by enabling organizations to audit and log security related events through inspection of email traffic between and within an organization including: communications or links to suspicious/malicious endpoints, suspicious/malicious email traffic, and infected files. Logs include, time stamps, source and destination addresses, identifiers, event descriptions, success/fail indications, rules involved. Security event information can be integrated with an organization's syslog server or SIEM product. Audit log events include:</p> <ul style="list-style-type: none"> Email System / Service / License status changes; DDI system settings; Mail system settings; Syslog and related settings; Integrated security products and related services settings; Detected suspicious events; Scanning / Analysis of audit logs; System maintenance activities; Account management; and

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
AU-2 Audit Events (Continued: Deep Security)		<ul style="list-style-type: none"> Audit log alerts and other actions. <p>Audit functionality for DDEI are very similar that described above for DDI.</p> <p>Deep Security (DS) supports compliance with the AU-2 and AU-3 requirements by enabling organizations to audit and log security related events through inspection of host-based network traffic for malicious activity, key files for changes, and system logs for indicators of suspicious activity. Audit records and Logs include for example: time stamps, source and destination addresses, identifiers, event descriptions, success/fail indications, rules involved. Security event information can be integrated with sys logs servers and an organization's selected SIEM product. Audit log events include:</p> <ul style="list-style-type: none"> Start-up and shutdown of audit functions; Access to Systems; Access to DS - Object IDs, Requested access; Reading of information from audit records; Unsuccessful attempts to read information from audit records; All modifications to the audit configuration that occur while the audit collection functions are operating; All use of the authentication mechanism - User identity, location; All use of the user identification mechanism - User identity, location; All modifications in the behavior of the functions of DS security functions; All modifications to the values of DS security function data Modifications to the group of users that are part of a role - User identity; and Use of the management functions - Where modified: data storage parameters, user identification and authentication attributes, user role attributes. <p>DS Audit functionality includes:</p> <ul style="list-style-type: none"> <u>Audit Review</u> - Authorized administrators can only review audit information which they have been granted access permissions. Information from audit records are provided in a manner suitable for authorized users to interpret the information. <u>Restricted audit review</u> - All users read access to the audit records is prohibited, except those users that have been granted explicit read-access. <u>Selectable audit review</u> - DS provides the ability to perform sorting of audit data based on date and time, type of event, event ID, event name, target system identity and event originator. <u>Selective audit</u> - Sets of events to be audited can be selected from the set of all auditable events based on the event attributes; <u>Guarantees of audit data availability</u> - The stored audit records are protected from unauthorized deletion and modifications. In addition, previously recorded audit records will be maintained during system attacks and failures.
AU-2 Audit Events (Continued: TippingPoint)		<p>TippingPoint The Audit log tracks user activity that might have security implications, including user attempts (successful and unsuccessful) to do the following:</p> <ul style="list-style-type: none"> - Change user information - Change IPS, routing or network configuration - Gain access to controlled areas (including the audit log) - Update system software and attack protection filter packages - Change filter settings <p>In addition the SMS features a policy-based operational model for scalable and uniform enterprise management. It enables behavior and performance analysis with trending reports, correlation and real-time graphs. Reporting includes all, specific, and top attacks and their sources and destinations, as well as all, specific, and top peers and filters for misuse and abuse (peer-to-peer piracy) attacks. An organization can create, save, and schedule reports using report templates. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. An organization can modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention.</p>

AU-2 Audit Events (Continued: Common Criteria evaluation)			<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-2 and AU-3 controls:</p> <ul style="list-style-type: none"> - FAU_GEN.1 (<i>Security Audit/ Security Audit Data Generation</i>).
--	--	--	--

AU-3 Audit and Accountability / Content of Audit Records

AU-3 Content of Audit Records The system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user or process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results, for example, the security and privacy state of the system after the event occurred. Related Controls: AU-2, AU-8, AU-12, AU-14, MA-4, SI-7, SI-11. References: NIST Interagency Report 8062.	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P	See responses to AU-2
AU-3 (1) Content of Audit Records / Additional Audit Information Generate audit records containing the following additional information: [Assignment: organization defined additional, more detailed information]. Supplemental Guidance: Implementation of this control enhancement is dependent on system functionality to configure audit record content. Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P	<p>Deep Discovery Inspector, Detection Logs can be queried for additional information, by detection types (Threats, Disruptive Applications, Malicious URLs, Virtual Analysis, Correlated Incidents, and Custom Detections), and time range.</p> <p>Deep Discovery Inspector - is able to include or exclude auditable events from the set of audited events based on the event type, through Selective Audit. (FAU_SEL.1)</p> <p>Deep Security supports compliance with this requirement through the defined audit events and the ability to carry out specific queries against the audit records simplifying the ability to locate the information of interest. In addition, deep packet inspection permits the capture of event data, at the packet level, which can be analyzed for additional audit data relating to the security event</p> <p>Deep Security is able to include or exclude auditable events from the set of audited events based on the event type, through Selective Audit (FAU_SEL.1)</p> <p>TippingPoint can support this requirement through configuration of the Audit log which tracks user activity that might have security implications, including user attempts (successful and unsuccessful) to do the following:</p> <ul style="list-style-type: none"> - Change user information - Change IPS, routing or network configuration - Gain access to controlled areas (including the audit log) - Update system software and attack protection filter packages - Change filter settings <p>Only users with Super-user access level can view, print, reset, and download the Audit log.</p> <p>To maintain a complete history of entries and provide a backup, the IPS device can be configured to send audit log entries to a remote syslog server from the Syslog Servers page.</p> <p>TippingPoint audit log entry contains the following fields:</p> <ul style="list-style-type: none"> - Log ID - The system-assigned log ID number. - Log EntryTime - A date and time stamp. - User - The login name of the user who performed the audited action. The user listed for an event can include SMS, SYS, and CLI. - Access - The access level of the user performing the action.

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
AU-3 (1) Content of Audit Records / Additional Audit Information (... Continued.)		<ul style="list-style-type: none"> - IP Address - The IP address from which the user performed the action. - Interface - The interface with which the user logged in: WEB for the LSM, CLI for the command line interface. For system-initiated actions, SYS displays in this field. - Component - The area in which the user perform an action (LOGIN, LOGOUT, and Launch Bar Tabs). - Result - The action performed or the result of a LOGIN or LOGOUT attempt. - Action - The action performed as a result. For example, Log Files Reset. <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>“provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.”</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC <u>Security Targets</u> includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-3 (1) control:</p> <ul style="list-style-type: none"> - FAU_GEN.1 (<i>Security Audit/ Security Audit Data Generation</i>).
AU-3 (2) Content of Audit Records / Centralized Management of Planned Audit Record Content Provide centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined system components]. Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the system. Related Controls: AU-6, AU-7.	H CNSSI 800-82 ICS 800-171 CU	E P <ul style="list-style-type: none"> Deep Discovery Inspector transports log content to syslog servers for central management using the following channels: <ul style="list-style-type: none"> - Transmission Control Protocol (TCP) - Transmission Control Protocol (TCP) with Secure Sockets Layer (SSL) encryption - User Datagram Protocol (UDP) Deep Discovery Inspector can be configured to send log content to a syslog server for centralized management in the following formats: <ul style="list-style-type: none"> - Common Event Format (CEF) - Log Event Extended Format (LEEF) - Trend Micro Event Format (TMEF) Deep Discovery Inspector, Management Console provides a built-in online capability through which users can view system status, configure threat detection, configure and view logs, run reports, and administer Deep Discovery Inspector. Deep Discovery Inspector can send suspicious objects and C&C callback addresses to TippingPoint centralized Security Management System (SMS) with various optional information. Deep Discover Email Inspector through the Trend Micro Control Manager which is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for managed products and services throughout the network. Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Control Manager allows both manual and prescheduled updates, and the configuration and administration of products as groups or as individuals for added flexibility. Deep Discovery Email Inspector Management Console provides a product centralized management capability for the audit logs Deep Security when integrated with the Trend Micro Control Manager support this requirement by providing centralized management and configuration of security events, rules and policies. Event information can be integrated with an organization's SIEM product. Deep Security through the centralized control of the Deep Security Manager supports the satisfying of this requirement for the audit event management and configuration. TippingPoint - The TippingPoint SMS Server is an enterprise-class management platform that provides centralized management, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices. Reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. These filters can be modified, updated, and control of the filter distribution according to segment groups for refined intrusion prevention. To maintain a complete

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
			history of entries and provide a backup, the TippingPoint IPS device can be configured to send audit log entries to a remote syslog server from the Syslog Servers page.
AU-4 Audit and Accountability / Audit Storage Capacity			
<p>AU-4 Audit Storage Capacity Allocate audit record storage capacity to accommodate [Assignment: organization-defined audit record retention requirements].</p> <p>Supplemental Guidance: Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.</p> <p>Related Controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.</p>	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector through the guarantee of audit data availability and the prevention of audit data loss ensures that if there is insufficient audit storage capacity the latest audit records are maintained and the organization is alerted to the issue.</p> <p>Guarantees of Audit Data Availability - protects the stored audit records from unauthorized deletion. Prevents modifications to the audit records, and ensure that the latest recorded audit records will be maintained when audit storage is exhausted.(FAU_STG.2)</p> <p>Prevention of Audit Data Loss - overwrites the oldest stored audit records and sends an alarm if the audit trail is full.(FAU_STG.4)</p> <p>Deep Security satisfies this requirement by monitoring the disk space available for logs and audit records, should free disk space fall below a threshold level alerts will be issued and audit /log data collected will be stored in temporary memory at the agent until sufficient free disk space is available.</p> <p>Deep Security through the guarantee of audit data availability and the prevention of audit data loss ensures that if there is insufficient audit storage capacity the latest audit records are maintained and the organization is alerted to the issue.</p> <p>Guarantees of audit data availability (FAU_STG.2) - protects the stored audit records from unauthorized deletion.(FAU_STG.2.1) and is able to prevent modifications to the audit records.(FAU_STG.2.2).Also, ensures that the previously recorded audit records will be maintained when failure and attack occur.(FAU_STG.2.3).</p> <p>Prevention of audit data loss (FAU_STG.4) - prevents auditable events, except those taken by the authorized user with special rights and send an alarm if the audit trail is full.</p> <p>TippingPoint maintains an historical log file and a current log file for each log. When the current log file reaches the default size (4MB), the log is de-activated and saved as the historical file, and a new log file is started as the current log. If a historical file already exists, that file is deleted. When the log is rolled over, the system generates a message in the Audit log. To save all log data and create a backup, the system can be configured to offload log messages to a remote system log. When the space available for audit storage is exhausted, the oldest 50% of audit records are deleted and an audit record to this effect is generated. The TippingPoint solution through the guarantee of audit data availability and the prevention of audit data loss ensures that if there is insufficient audit storage capacity the latest audit records are maintained and the organization is alerted to the issue.</p> <p>In addition SMS has the ability to automatically forward the IPS Audit log entries via syslog.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-4 control:</p> <ul style="list-style-type: none"> - FAU_STG.4 (Security Audit/ Security Audit Event Storage/ Prevention of Audit Data Loss). <p>In addition, guarantees of Audit Data Availability (FAU_STG.2) protects the stored audit records in the audit trail from unauthorized deletion FAU_STG.2.1 and is able to prevent unauthorized modifications to the stored audit records in the audit trail. (FAU_STG.2.2). Also, ensures that the most recent 50% of stored audit records will be maintained when audit storage exhaustion.(FAU_STG.2.3)</p> <p>Prevention of Audit Data Loss (FAU_STG.4) overwrites the oldest stored audit records and sends an alarm if the audit trail is full. (FAU_STG.4.1)</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
---------------------------	----------	---------	---------------------------------

AU-5 Audit and Accountability / Response to Audit Processing Failures

<p>AU-5 Audit and Accountability / Response to Audit Processing Failures</p> <p>a. Alert [Assignment: organization-defined personnel or roles] in the event of an audit processing failure within [Assignment: organization-defined time-period]; and</p> <p>b. Take the following additional actions: [Assignment: organization-defined actions to be taken].</p> <p>Supplemental Guidance: Organization-defined actions include, for example, shutting down the system; overwriting oldest audit records; and stopping the generation of audit records. Examples of audit processing failures include, for example, software and hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for audit processing failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. This control applies to each audit data storage repository (i.e., distinct system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.</p> <p>Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.</p>	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-5 control:</p> <ul style="list-style-type: none"> - FAU_STG.4 (Security Audit/ Security Audit Event Storage/ Prevention of Audit Data Loss). <p>-----</p> <p>Deep Discovery Inspector – addresses this requirement through prevention of Audit Data Loss (FAU_STG.4) by overwriting the oldest stored audit records and sending an alarm if the audit trail is full.</p> <p>Deep Discovery Inspector ensures that the latest recorded audit records will be maintained when audit storage exhaustion occurs (FAU_STG.2.3).</p> <p>Deep Security addresses this requirement through the Prevention of audit data loss (FAU_STG.4) by preventing auditable events, except those taken by the authorized user with special rights and send an alarm if the audit trail is full.</p> <p>Deep Security ensures that the previously recorded audit records will be maintained when failure and attack occur.</p> <p>TippingPoint address this requirement through Prevention of Audit Data Loss (FAU_STG.4). TippingPoint overwrites the oldest stored audit records and sends an alarm if the audit trail is full. The SMS has the capability to automatically forward the IPS Audit log entries via syslog.</p>
<p>AU-5 (1) Response to Audit Processing Failures / Audit Storage Capacity</p> <p>Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time-period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.</p> <p>Supplemental Guidance: Organizations may have multiple audit data storage repositories distributed across multiple system components, with each repository having different storage volume capacities.</p>	<p>H</p> <p>CNSSI 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector through the guarantee of audit data availability and the prevention of audit data loss ensures that if there is insufficient audit storage capacity the latest audit records are maintained and the organization is alerted to the issue.</p> <p>Specifically, Deep Discovery Inspector – addresses this requirement through:</p> <p>Prevention of Audit Data Loss (FAU_STG.4) by overwriting the oldest stored audit records and sending an alarm if the audit trail is full.</p> <p>Deep Security can satisfy this requirement by monitoring the disk space available for logs and audit records, should free disk space fall below a threshold level alerts will be issued and audit /log data collected will be stored in temporary memory at the agent until sufficient free disk space is available.</p> <p>Deep Security prevention of audit data loss (FAU_STG.4) prevents auditable events, except those taken by the authorized user with special rights and sends an alarm if the audit trail is full. In addition, Auditable events in general shall be prevented upon detection of a full audit trail. For unpreventable events, they shall be recorded by saving the events in temporary storage until space is made available and the events can be written to the database.</p> <p>TippingPoint though the guarantee of audit data availability (FAU_STG.2) ensures that the most recent 50% of stored audit records will be maintained when audit storage exhaustion occurs. Through the Prevention of Audit Data Loss (FAU_STG.4) it overwrites the oldest stored audit records and sends an alarm if the audit trail is full</p>
<p>AU-5 (1) Response to Audit Processing Failures / Audit Storage Capacity</p> <p>Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time-period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.</p> <p>Supplemental Guidance: Organizations may have multiple audit data storage repositories distributed across multiple system components, with each repository having different storage volume capacities.</p>	<p>H</p> <p>CNSSI 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector through the guarantee of audit data availability and the prevention of audit data loss ensures that if there is insufficient audit storage capacity the latest audit records are maintained and the organization is alerted to the issue.</p> <p>Specifically, Deep Discovery Inspector – addresses this requirement through:</p> <p>Prevention of Audit Data Loss (FAU_STG.4) by overwriting the oldest stored audit records and sending an alarm if the audit trail is full.</p> <p>Deep Security can satisfy this requirement by monitoring the disk space available for logs and audit records, should free disk space fall below a threshold level alerts will be issued and audit /log data collected will be stored in temporary memory at the agent until sufficient free disk space is available.</p> <p>Deep Security prevention of audit data loss (FAU_STG.4) prevents auditable events, except those taken by the authorized user with special rights and sends an alarm if the audit trail is full. In addition, Auditable events in general shall be prevented upon detection of a full audit trail. For unpreventable events, they shall be recorded by saving the events in temporary storage until space is made available and the events can be written to the database.</p> <p>TippingPoint though the guarantee of audit data availability (FAU_STG.2) ensures that the most recent 50% of stored audit records will be maintained when audit storage exhaustion occurs. Through the Prevention of Audit Data Loss (FAU_STG.4) it overwrites the oldest stored audit records and sends an alarm if the audit trail is full</p>

AU-6 Audit and Accountability / Audit Review, Analysis and Reporting

<p>AU-6 Audit Review, Analysis, and Reporting</p> <p>a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity];</p> <p>b. Report findings to [Assignment: organization-defined personnel or roles]; and</p>	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E</p>	<p>Deep Discovery Inspector can assist in meeting this control requirement through the Retro Scan Service, which scans historical web access logs (audit) for callback attempts to Command & Control(C&C) servers and other related activities in a network. Web access logs may contain undetected and unblocked connections to C&C servers that have only recently been discovered. Examination of such logs is an important part of forensic investigations to determine if the organizations network is affected by attacks. Deep Discovery Inspector forwards suspicious events to a centralized logging server for further correlation, reporting and archiving.</p>
---	--	----------	---

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>c. Adjust the level of audit review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.</p> <p>Supplemental Guidance: Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system boundaries, and use of mobile code or VoIP. Findings can be reported to organizational entities that include, for example, the incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities, the review/analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.</p> <p>Related Controls: AC-2, AC-3, AC-6, AC-7, AC-17, AU-7, AU-16, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SC-7, SI-3, SI-4, SI-7.</p> <p>References: NIST Special Publications 800-86, 800-101.</p>			<p>Deep Discovery Email Inspector -Tracks any email message that passed through Deep Discovery Email Inspector, including blocked and delivered messages. Deep Discovery Email Inspector records message details, including the sender, recipients, and the taken policy action. Message tracking logs indicate if an email message was received or sent by Deep Discovery Email Inspector. Message tracking logs also provide evidence about Deep Discovery Email Inspector investigating an email message.</p> <p>Deep Security Log Inspection capability provides visibility into important security events buried in log files, and creates audit trails of administrator activity. Optimizes the identification of important security events buried in multiple log entries across the data center. Forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving.</p> <p>Deep Security also maintains information regarding the administration and management of its security functions as part of the audit records.</p> <p>TippingPoint monitors and reports on events which monitor system performance and review traffic-related events. The following options are available:</p> <ul style="list-style-type: none"> - Logs — View information on system events and traffic-related events triggered by IPS filters and policies. Logs include alert, quarantine, block, audit, and system logs. - Managed Streams — Review and manage traffic streams that have been blocked, rate-limited, trusted, or quarantined by IPS policies. Manually quarantine or release a quarantined IP address. - Health — Review the current status and network performance of the IPS device. Information includes memory and disk usage statistics, status of the Threat Suppression Engine and the Ethernet ports, and throughput performance. - Reports —View graphs showing information on traffic flow, traffic-related events, and statistics on triggered filters (filter matches, rate limit, traffic, DDoS, quarantine, and adaptive filter).
<p>AU-6 (1) Audit Review, Analysis, and Reporting / Process Integration</p> <p>Employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.</p> <p>Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits.</p> <p>Related Controls: PM-7.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Discovery Inspector employs continuous monitoring of threat detections, which includes information on: Malicious Content, Malicious Behavior, Suspicious Behavior, Exploits, Grayware, Web Reputation, and Disruptive Applications. This threat data can be sent to a centralized logging server for correlation, reporting and archiving with audit record data to support organizational processes for investigation and response to suspicious activities.</p> <p>Deep Security, Recommendation Scan supports this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits. Deep Security further supports this integration of audit capabilities through the audit management functionality of the Deep Security Manager.</p> <p>TippingPoint automatically monitors and reports on events which monitor system performance and review traffic-related events. The following options are available:</p> <ul style="list-style-type: none"> - Logs — View information on system events and traffic-related events triggered by IPS filters and policies. Logs include alert, quarantine, block, audit, and system logs. - Managed Streams — Review and manage traffic streams that have been blocked, rate-limited, trusted, or quarantined by IPS policies. Manually quarantine or release a quarantined IP address. - Health — Review the current status and network performance of the IPS device. Information includes memory and disk usage statistics, status of the Threat Suppression Engine and the Ethernet ports, and throughput performance. - Reports —View graphs showing information on traffic flow, traffic-related events, and statistics on triggered filters (filter matches, rate limit, traffic, DDoS, quarantine, and adaptive filter).
<p>AU-6 (3) Audit Review, Analysis, and Reporting / Correlate Audit Repositories</p> <p>Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.</p> <p>Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and system) and supports cross-organization awareness.</p> <p>Related Controls: AU-12, IR-4.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Discovery Inspector supports the ability to correlate audit data by providing interfaces to the Trend Micro Control Manager and either a syslog server or input directly to an SIEM system to provide organization awareness across all tiers of the organization.</p> <p>Deep Discovery Email Inspector is integrated with the Trend Micro Control Manager which is a software management solution that provides the ability to control antivirus and content security programs from a central location, regardless of the program's physical location or platform. This application can correlate and simplify the administration of a corporate antivirus and content security policy. The Control Manager provides Log Aggregation Settings, Suspicious object data aggregation, Reports- One-time Reports</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
AU-6 (3) Audit Review, Analysis, and Reporting / Correlate Audit Repositories (... Continued.)		<p>and Scheduled Reports; and Notifications Events.</p> <p>Deep Security supports the ability to correlate audit data by providing interfaces to the Trend Micro Control Manager and either a syslog server or input directly to an SIEM system to provide organization awareness across all tiers of the organization.</p> <p>TippingPoint supports this control through the use of the Security Management System (SMS) an enterprise-class management platform that provides a correlated and centralized administration, configuration, monitoring and reporting providing situational awareness for well over a hundred TippingPoint IPS devices. The SMS provides the following functionality:</p> <ul style="list-style-type: none"> - Enterprise-wide device status and behavior monitoring — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status. - IPS networking and configuration — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group. - Filter customization — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings. - Filter and software distribution — Monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS client. The SMS client and Central Management Server can distribute these packages according to segment group settings. The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates.
AU-6 (4) Audit Review, Analysis, and Reporting / Central Review and Analysis Provide and implement the capability to centrally review and analyze audit records from multiple components within the system. Supplemental Guidance: Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products. Related Controls: AU-2, AU-12.	CNSSI FedRAMP 800-171 CUI	E <p>Deep Discovery Inspector supports the ability to centrally review and analyze audit data by providing interfaces to the Trend Micro Control Manager and either a syslog server or input directly to an SIEM system. Deep Discovery Inspector, also provides a centralized management, analysis and review capabilities Management Console provides a built-in online capability through which users can view system status, configure threat detection, configure and view logs, run reports, and administer Deep Discovery Inspector.</p> <p>Deep Discovery Email Inspector supports this central review and analysis control through the integration of the Trend Micro Control Manager. Control Manager allows system administrators to monitor audit logs and report on activities such as infections, security violations, or virus entry points. Deep Discovery Email Inspector also provides a built-in management console that can be used to configure and manage the product</p> <p>Deep Security through the centralized control of the Deep Security Manager supports the satisfying of this requirement for the audit event management and configuration. In addition, supports the ability to centrally review and analyze audit data by providing interfaces to the Trend Micro Control Manager and either a syslog server or input directly to an SIEM system</p> <p>TippingPoint supports the central review and analysis control through the Security Management System (SMS) Server which is an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices. The SMS provides enterprise-wide device status and behavior monitoring — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status.</p>
AU-6 (5) Audit Review, Analysis, and Reporting / Integration / Scanning and Monitoring Capabilities Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity. Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple system components as	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E <p>Deep Discovery Inspector can support the ability to scan and monitor audit data for threat detection data, by providing interfaces to either a syslog server or input directly to an Security Event and Information Management (SEIM) system to enhance the ability to identify inappropriate or unusual activity. Deep Discovery Inspector also offers administrators the option to include Trend Micro Retro Scan as part of the Smart Protection Network. Retro Scan is a cloud-based service that scans historical web access logs for callback attempts to C&C servers and other related activities in a network. Web access logs may contain undetected and unblocked connections to C&C servers that have only recently been discovered</p> <p>Deep Discovery Email Inspector message tracking logs provide evidence about Deep Discovery Email Inspector investigating an email message which shows all email messages with malicious and suspicious characteristics. Suspicious characteristics include anomalous behavior, false or misleading data, suspicious and malicious behavior</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can uncover denial of service attacks or other types of attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.</p> <p>Related Controls: AU-12, IR-4.</p>		<p>patterns, and strings that indicate system compromise but require further investigation. Email Messages with Advanced Threats is available in Control Manager, which aggregates data from several Deep Discovery Email Inspector appliances.</p> <p>Deep Security, Log Inspection capability provides scanning and visibility into important security events buried in log files, and creates audit trails of administrator activity. Optimizes the identification of important security events buried in multiple log entries across the data center. Forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving.</p> <p>TippingPoint automatically scans, monitors and reports on events which monitor system performance and review traffic-related events. The following options are available:</p> <ul style="list-style-type: none"> - Logs — View information on system events and traffic-related events triggered by IPS filters and policies. Logs include alert, quarantine, block, audit, and system logs. - Managed Streams — Review and manage traffic streams that have been blocked, rate-limited, trusted, or quarantined by IPS policies. Manually quarantine or release a quarantined IP address. - Health — Review the current status and network performance of the IPS device. Information includes memory and disk usage statistics, status of the Threat Suppression Engine and the Ethernet ports, and throughput performance. - Reports —View graphs showing information on traffic flow, traffic-related events, and statistics on triggered filters (filter matches, rate limit, traffic, DDoS, quarantine, and adaptive filter).
<p>AU-6 (7) Audit and Accountability / Audit Review, Analysis, and Reporting / Permitted Actions</p> <p>Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit information.</p> <p>Supplemental Guidance: Organizations specify permitted actions for system processes, roles, and/or users associated with the review, analysis, and reporting of audit records through account management techniques. Specifying permitted actions on audit information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include, for example, read, write, execute, append, and delete.</p>	<p>FedRAMP 800-171 CUI</p>	<p>P</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-6 (7) control:</p> <ul style="list-style-type: none"> - FMT_MTD.1 (Security Management/ Management of TSF Data). <p>---</p> <p>Deep Discovery Inspector provides this control capability through the Common Criteria, Security Target and the Management of Deep Discovery Inspector security function data (FMT_MTD.1) Deep Discovery Inspector restricts the ability to query and add System and audit data, and shall restrict the ability to query and modify all other Deep Discovery Inspector data to the authorized System administrators and authorized administrators.</p> <p>Deep Security provides this control capability through the Common Criteria Security Target and the management of Deep Security, security functions data (FMT_MTD.1a) Deep Security restricts the ability to query and add System and audit data, and restricts the ability to query and modify all other Deep Security data to the Full Access role.</p> <p>Deep Security allows additional roles to be defined (by authorized administrators with sufficient privileges) that grant the ability to query and modify a sub-set of System data. This control capability is also provided through the management of Deep Security security functions data (FMT_MTD.1b) Deep Security restricts the ability to query audit data and all other Deep Security data to the Full Access role and Auditor role.</p> <p>By default, the “Full Access” and “Auditor” roles have read-only access to all of the audit records. The default configuration “Auditor” role has the ability to query audit data and other Deep Security data but not to modify it as in FMT_MTD.1a. Deep Security allows other roles to be defined (by authorized administrators with sufficient privileges) that grant the ability to query a sub-set of System data.</p> <p>TippingPoint provides this control capability through the Common Criteria Security Target and the management of TippingPoint Security Function data (FMT_MTD.1). TippingPoint restricts the following actions to Super-user administrators:</p> <ul style="list-style-type: none"> - Modify the: Failed Login Action; Security Level; the users' passwords; and System time; - Modify, delete, create the User accounts; - Modify, delete, create the: Traffic management filters; Notification contacts; Inspection bypass rules; - Modify the set of audited events to Super-user, Administrator;

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
			<ul style="list-style-type: none"> - Clear the audit trail; and - Clear the DS data.
AU-7 Audit and Accountability / Audit Reduction and Report Generation			
<p>AU-7 Audit Reduction and Report Generation</p> <p>Provide and implement an audit reduction and report generation capability that:</p> <ul style="list-style-type: none"> a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records. <p>Supplemental Guidance:</p> <p>Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.</p> <p>Related Controls: AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM12, SI-4.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AU-7 control:</p> <ul style="list-style-type: none"> - FAU_SAR.1 (Security Audit Review/ Audit Review); - FAU_SAR.3 (Security Audit Review/ Selectable Audit Review). <p>----</p> <p>Deep Discovery Inspector assists with audit reduction and report generation through the ability to configure an "audit event". Administrators have the ability to modify the granularity of the type and frequency of audit events to be recorded and collected. Deep Discovery Inspector has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Selectable Audit Review" and "Selective Audit" is confirmed through the Audit Review capability (FAU_SAR.1). This Deep Discovery Inspector Security Function provides authorized System administrators and authorized administrators with the capability to read all audit information as specified in the audit records. Deep Discovery Inspector Security Functions provide the audit records in a manner suitable for the user to interpret the information. Deep Discovery Inspector Administrators with the default configuration role of "authorized system administrator" and "authorized administrator" are granted access to all Deep Discovery Inspector audit records. Through Restricted Audit Review (FAU_SAR.2) Deep Discovery Inspector prohibits all users read access to the audit records, except those users that have been granted explicit read-access. Also through Selectable Audit Review (FAU_SAR.3) Deep Discovery Inspector provides the ability to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event..</p> <p>Deep Security assists with audit reduction and report generation through the ability to configure an "audit event". Administrators have the ability to modify the granularity of the type and frequency of audit events to be recorded and collected. Deep Security has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Selectable Audit Review" and "Selective Audit" is confirmed through the Audit Review capability (FAU_SAR.1). Deep Security provides authorized administrators with the capability to read audit information which they have been granted access to from the audit records. Deep Security provides the audit records in a manner suitable for the user to interpret the information. Deep Security Administrators with the default configuration roles named "Full Access" and "Auditor" are granted access to all Deep Security audit records. Deep Security Restricted audit review prohibits all users read access to the audit records, except those users that have been granted explicit read-access. Deep Security Selectable audit review provides the ability to perform sorting of audit data based on date and time, type of event, event ID, event name, target system identity and event originator.</p> <p>TippingPoint assists with audit reduction and report generation through the ability to search through audit logs for specific criteria, such as date range, protocol, source port, etc. TippingPoint has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Audit Review and Selective Audit is confirmed through the:</p> <p>Audit Review capability (FAU_SAR.1). TippingPoint provides the Super-user role with the capability to read all auditable events that are recorded] from the audit records.</p> <p>TippingPoint provides the audit records in a manner suitable for the user to interpret the information. Selectable Audit Review (FAU_SAR.3) as implemented in TippingPoint provides the ability to apply sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event.</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>AU-7 (1) Audit Reduction and Report Generation / Automatic Processing</p> <p>Provide and implement the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].</p> <p>Supplemental Guidance: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, Internet Protocol addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location or selectable by specific system component.</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-7 (1) control:</p> <ul style="list-style-type: none"> - FAU_SAR.3 (Security Audit Review/ Selectable Audit Review). <p>---</p> <p>Deep Discovery Inspector supports this capability of processing audit records for events of interest by providing the ability to search through the audit records based on event criteria, such as event location, event type, date and times, and identities of individuals. This can be used to provide a reduced subset of the audit records that are of special interest to the organization. In addition, Deep Discovery Inspector has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Selectable Audit Review (FAU_SAR.3). Deep Discovery Inspector provides the ability to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event.</p> <p>Deep Security supports this capability by providing the ability to search through the audit records based on event location, event type, date and times, and identities of individuals. This can be used to provide a reduced subset of the audit records that are of special interest to the organization. In addition, Deep Security has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Selectable Audit Review (FAU_SAR.3). Deep Security provides the ability to perform sorting of audit data based on date and time, type of event, event ID, event name, target system identity and event originator.</p> <p>Deep Security, Log Inspection capability provides support for this control at the enterprise level through scanning and visibility into important security events buried in log files, and creating audit trails of administrator activity, optimizes the identification of important security events buried in multiple log entries across the data center. Deep Security forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving.</p> <p>TippingPoint has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Selectable Audit Review (FAU_SAR.3), which provides the ability to apply sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event.</p>
<p>AU-7 (2) Audit Reduction and Report Generation / Automatic Sort and Search</p> <p>Provide and implement the capability to sort and search audit records for events of interest based on the content of [Assignment: organization-defined audit fields within audit records].</p> <p>Supplemental Guidance: Sorting and searching of audit records may be based upon the contents of audit record fields, for example, date and time of events; user identifiers; Internet Protocol addresses involved in the event; type of event; or event success or failure.</p>	<p>800-171 CUI</p>	<p>E P</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-7 (2) control:</p> <ul style="list-style-type: none"> - FAU_SAR.3 (Security Audit Review/ Selectable Audit Review). <p>---</p> <p>Deep Discovery Inspector supports this capability of sorting and searching audit records for events of interest by providing the ability to search through the audit records based on event criteria, such as event location, event type, date and times, and identities of individuals. This can be used to provide a reduced subset of the audit records that are of special interest to the organization. In addition, Deep Discovery Inspector has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Selectable Audit Review (FAU_SAR.3). Deep Discovery Inspector provides the ability to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event.</p>

AU-7 (2) Audit Reduction and Report Generation / Automatic Sort and Search (... Continued.)			<p>Deep Security supports this capability by providing the ability to search through the audit records based on event location, event type, date and times, and identities of individuals. This can be used to provide a reduced subset of the audit records that are of special interest to the organization. In addition, Deep Security has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Selectable Audit Review (FAU_SAR.3). Deep Security provides the ability to perform sorting of audit data based on date and time, type of event, event ID, event name, target system identity and event originator.</p> <p>Deep Security, Log Inspection capability provides support for this control at the enterprise level through scanning and visibility into important security events buried in log files, and creating audit trails of administrator activity, optimizes the identification of important security events buried in multiple log entries across the data center. Deep Security forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving.</p> <p>TippingPoint has been certified by the Common Criteria Evaluation and Certification Scheme providing evidence of the capability for Selectable Audit Review (FAU_SAR.3), which provides the ability to apply sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event. TippingPoint is able to provide reliable time stamps (FPT_STM.1).</p>
--	--	--	---

AU-8 Audit and Accountability / Time Stamps

AU-8 Audit and Accountability / Time Stamps a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that can be mapped to Coordinated Universal Time or Greenwich Mean Time and meets [Assignment: organization-defined granularity of time measurement]. Supplemental Guidance: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related Controls: AU-3, AU-12, AU-14.	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector uses the Network Time Protocol (NTP) which synchronizes computer system clocks across the Internet. The NTP settings can be configured to synchronize the server clock with an NTP server, or manually set the system time.</p> <p>Peep Discovery Email Inspector uses the Network Time Protocol (NTP) which synchronizes computer system clocks across the Internet. The NTP settings can be configured to synchronize the server clock with an NTP server, or manually set the system time. Deep Discovery Email Inspector sorts logs using UTC 0 time, even if the display is in local time.</p> <p>Deep Discovery Analyzer uses the Network Time Protocol (NTP) which synchronizes computer system clocks across the Internet. The NTP settings can be configured to synchronize the server clock with an NTP server, or manually set the system time.</p> <p>Deep Security uses NTP for reliable timestamps. The system time on the Deep Security Manager operating system is synchronized with the time on the database computer. An alert appears in the Alert Status widget of the manager console when the computer times are more than 30 seconds out of sync.</p> <p>TippingPoint is able to provide reliable time stamps (FPT_STM.1)</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-8 control: - FPT_STM.1 (Protection of the TSF/time Stamps / Reliable Time Stamps).</p>
--	--	---	--

AU-9 Audit and Accountability / Protection of Audit Information

AU-9 Protection of Audit Information Protect audit information and audit tools from unauthorized access, modification, and deletion. Supplemental Guidance: Audit information includes all information, for example, audit records, audit settings, audit reports, and personally identifiable information, needed to successfully audit system	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector, Deep Security and TippingPoint protect audit information from unauthorized access, modification, and deletion. This has been demonstrated by the Common Criteria process as indicated in the products Security Target.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p>
---	--	---	--

<p>activity. This control focuses on technical or automated protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.</p> <p>Related Controls: AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SC8, SI-4.</p> <p>References: FIPS Publications 140-2, 180-4, 202</p>			<p><i>(Common Criteria) to the controls in NIST Special Publication 800-53.</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC <u>Security Targets</u> include the following control which is mapped (in SP 800-53 Table I-3) to supporting the AU-9 control:</p> <ul style="list-style-type: none"> - FAU_STG.2 (Security Audit/ Security Audit Event Storage/ Guarantee of Audit Data Availability).
<p>AU-9 (2) Protection of Audit Information / Audit Backup on Separate Physical Systems / Components</p> <p>Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.</p> <p>Supplemental Guidance:</p> <p>Storing audit information in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. It may also enable management of audit records as an organization-wide activity. This control enhancement applies to initial generation as well as backup or long-term storage of audit information.</p> <p>Related Controls: AU-4, AU-5.</p>	<p>H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p>	<p>Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, Deep Security, TippingPoint support this capability through the ability to transmit the audit and log files to a syslog server or to a SIEM type system. Deep Security supports this control by storing log data in the Deep Security Manager database, which is independent of the system being monitored.</p> <p>Further, authorized administrators can only read audit records through the administrative interface and their access rights to the audit records is restricted based on their role definition. No administrator is given write access to the audit records</p>
<p>AU-9 (4) Protection of Audit Information / Access by Subset of Privileged Users</p> <p>Authorize access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].</p> <p>Supplemental Guidance:</p> <p>Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.</p> <p>Related Controls: AC-5.</p> <p>AU-9 (6) Protection of Audit Information / Read-Only Access</p> <p>Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users].</p> <p>Supplemental Guidance:</p> <p>Restricting privileged user authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users, for example, deleting audit records to cover up malicious activity.</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p> <p>800-171 CUI</p>	<p>P</p> <p>P</p>	<p>Deep Discovery Inspector authorized administrators can only read audit records through the administrative interface; access rights to the audit records are restricted based on their role definition. No administrator is given write access to the audit records; therefore this prevents modifications to the audit records.</p> <p>Deep Security supports the satisfying of this requirement by providing only authorized administrators with the capability to read audit information, which they have been granted access to. Deep Security prohibits all users read access to the audit records, except those users that have been granted explicit read-access to the audit records.</p> <p>Deep Security through the "Auditor" role, gives the Auditor the ability to view all the information in the Deep Security system but not the ability to make any modifications except to their personal settings (password, contact information, view preferences, etc.).</p> <p>This capability has been demonstrated through the Common Criteria evaluation process: Deep Discovery Inspector, Deep Security and TippingPoint have been certified by the Common Criteria Evaluation and Certification Scheme to meet this control.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>"provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC <u>Security Targets</u> include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the AU-9 (4) and AU-9 (6) controls:</p> <ul style="list-style-type: none"> - FMT_MTD.1 (Security Management/ Management of TSF Data) – AU-9(4); - FAU_SAR.2 (Security Audit/ Security Audit Review/ Restricted Audit Review) – AU-9 (6).

AU-12 Audit and Accountability / Audit Generation

<p>AU-12 Audit Generation</p> <ol style="list-style-type: none"> Provide audit record generation capability for the auditable event types in AU-2 a. at [Assignment: organization-defined system components]; Allow [Assignment: organization-defined personnel or roles] to select which auditable event types are to be audited by specific components of the system; and Generate audit records for the event types defined in AU-2 d. with the content in AU-3. <p>Supplemental Guidance:</p> <p>Audit records can be generated from many different system components. The list of audited event types is the set of event types for which audits are to be generated. These</p>	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p>	<p>Deep Discovery Inspector, Deep Security, and TippingPoint have been certified by the Common Criteria Evaluation and Certification Scheme to meet this control requirement for audit data generation and selective audit by being able to generate an audit record of auditable events.</p> <p>At an enterprise level Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Security, and TippingPoint detect security events at the network, server and endpoints and create dashboard reports, which could be used by an auditor during an Audit Review of the organization's environment.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be</p>
--	--	------------	--

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>event types are a subset of all event types for which the system can generate audit records.</p> <p>Related Controls: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12 SC-18, SI-3, SI-4, SI-7, SI-10.</p>			<p>addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following control which are mapped (in SP 800-53 Table I-3) to supporting the AU-12 control:</p> <ul style="list-style-type: none"> - FAU_GEN.1 (Security Audit/ Security Audit Data Generation); - FAU_SEL.1 (Security Audit/ Audit Event Selection/ Selective Audit)
<p>AU-12 (1) Audit Generation / System-Wide / Time-Correlated Audit Trail</p> <p>Compile audit records from [Assignment: organization-defined system components] into a system wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization defined level of tolerance for the relationship between time stamps of individual records in the audit trail].</p> <p>Supplemental Guidance:</p> <p>Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.</p> <p>Related Controls: AU-8.</p>	H CNSSI 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Security, and TippingPoint support compliance with this requirement through the generation of date and time stamps which can be synchronized to an accurate, correct, and reliable time source, such as provided by the local IT environment or through a Network Time Protocol service.</p> <p>See AU-8 Timestamps.</p>
<p>AU-12 (2) Audit Generation / Standardized Formats</p> <p>Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.</p> <p>Supplemental Guidance:</p> <p>Audit information that is normalized to common standards promotes interoperability and exchange of such information between dissimilar devices and systems. This facilitates production of event information that can be more readily analyzed and correlated.</p> <p>Standard formats for audit records include, for example, system log records and audit records compliant with Common Event Expressions (CEE). If logging mechanisms within systems do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.</p>	800-171 CUI	E P	<p>Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, and Deep Security all permit the selection of the format in which audit/event logs can be sent to a remote syslog server.</p> <ul style="list-style-type: none"> - CEF: Common Event Format (CEF) is an open log management standard developed by HP ArcSight. CEF comprises a standard prefix and a variable extension that is formatted as key-value pairs. - LEEF: Log Event Extended Format (LEEF) is a customized event format for IBM Security QRadar. LEEF comprises an LEEF header, event attributes, and an optional syslog header. <p>TippingPoint makes use of RFC 3164. RFC format can be enabled for audit/event logs so that the remote syslog messages meet RFC requirements. This setting has no effect on the format of alert and block log remote syslog messages.</p>

CA-2 Security Assessment and Authorization / Security Assessments

<p>CA-2 Assessment, Authorization, and Monitoring / Assessments</p> <ol style="list-style-type: none"> a. Develop a security and privacy assessment plan that describes the scope of the assessment including: <ol style="list-style-type: none"> 1. Security and privacy controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Ensure the assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; c. Assess the security and privacy controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; d. Produce a security and privacy assessment report that document the results of the assessment; and e. Provide the results of the security and privacy control assessment to [Assignment: organization-defined individuals or roles]. <p>Supplemental Guidance:</p> <p>Organizations assess security and privacy controls in organizational systems and the environments in which those systems operate as part of initial and ongoing authorizations; FISMA annual assessments; continuous monitoring; and system development life cycle activities. Assessments ensure that organizations meet information security and privacy requirements; identify weaknesses and deficiencies in the development process; provide essential information needed to make risk-based decisions as part of authorization processes; and ensure compliance to vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls from Chapter Three as documented in security plans and privacy plans. Organizations can use other types of assessment</p>	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following control which are mapped (in SP 800-53 Table I-3) to supporting the CA-2 control:</p> <ul style="list-style-type: none"> - ATE_IND.2 (Tests/ Independent Testing/ Sample). <p>3E -- "The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified."</p>
--	--	---	--

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>activities such as vulnerability scanning and system monitoring to maintain the security and privacy posture of systems during the entire life cycle. Assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, and/or authorizing official designated representatives.</p> <p>To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations; continuous monitoring; or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits including, for example, audits by external entities such as regulatory agencies, are outside the scope of this control. Related Controls: AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SC-38, SI-3, SI-12.</p> <p>References: FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-122, 800-137; NIST Interagency Report 8062.</p>		
<p>CA-2 (1) Assessment, Authorization, and Monitoring / Assessments / Independent Assessors</p> <p>Employ independent assessors or assessment teams to conduct security and privacy control assessments.</p> <p>Supplemental Guidance: Independent assessors or assessment teams are individuals or groups conducting impartial assessments of systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors should not create a mutual or conflicting interest with the organizations where the assessments are being conducted; assess their own work; act as management or employees of the organizations they are serving; or place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals.</p> <p>Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted assessment services have sufficient independence, for example, when system owners are not directly involved in contracting processes or cannot influence the impartiality of assessors conducting assessments. When organizations that own the systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.</p>	M H CNSSI FedRAMP 800-82 ICS	P <p>Deep Discovery Inspector, Deep Security and TippingPoint through the Common Criteria certification process are subjected to Independent Testing and Assessment.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC <u>Security Targets</u> include the following control which are mapped (in SP 800-53 Table I-3) to supporting the CA-2 (1) control:</p> <ul style="list-style-type: none"> - ATE_IND.2 (Tests/ Independent Testing/ Sample).
<p>CA-2 (2) Security Assessments / Specialized Assessments</p> <p>Include as part of security and privacy control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; [Assignment: organization-defined other forms of assessment]].</p> <p>Supplemental Guidance: Organizations can conduct specialized assessments including, for example, verification,</p>	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P <p>Deep Discovery Inspector supports this requirement through reporting of malicious activity, files and suspicious behavior that can be used by assessors.</p> <p>Deep Discovery Email Inspector supports this control through Monitoring Rules a maximum of 10 monitoring rules can be used. The monitoring rules specify the SMTP traffic that Deep Discovery Email Inspector monitors for cyber threats.</p> <p>Deep Discovery Analyzer supports this requirement through the use of SNMP monitoring of devices attached to a network for conditions that merit administrative attention. The Advanced Threat Scan Engine protects against viruses, malware, and</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>validation, insider threat assessments, malicious user testing, system monitoring, and other forms of testing. Such assessments can improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security and privacy. Organizations conduct these types of specialized assessments in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes.</p> <p>Related Controls: PE-3, SI-2.</p>			<p>exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature based, behavior-based, and aggressive heuristic detection</p> <p>Deep Security uses multiple techniques to identify suspicious behavior. The anti-malware engine can identify suspicious programs or processes. Using Integrity Monitoring or Log Inspection can give early indicators of compromise. All of these capabilities can run in real-time or can be scheduled for regular scans. In addition the Recommendation scan can help support this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits.</p> <p>TippingPoint supports this control by providing scanning and system monitoring to protect the enterprise network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device.</p> <p>Further evidence to support this requirement, in terms of "Vulnerability Analysis" is provided by Deep Discovery Inspector, Deep Security, and TippingPoint as shown by the Common Criteria Evaluation and Certification Scheme.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following control which are mapped (in SP 800-53 Table I-3) to supporting the CA-2 (2) control:</p> <ul style="list-style-type: none"> - AVA_VAN.2 (<i>Vulnerability Assessment/ Vulnerability Analysis</i>).

CA-7 Security Assessment and Authorization / Continuous Monitoring

<p>CA-7 Security Assessment and Authorization / Continuous Monitoring</p> <p>Develop a security and privacy continuous monitoring strategy and implement security and privacy continuous monitoring programs that include:</p> <ol style="list-style-type: none"> Establishing the following security and privacy metrics to be monitored: [Assignment: organization-defined metrics]; Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for ongoing assessment of security and privacy control effectiveness; Ongoing security and privacy control assessments in accordance with the organizational continuous monitoring strategy; Ongoing security and privacy status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; Correlation and analysis of security- and privacy-related information generated by security and privacy control assessments and monitoring; Response actions to address results of the analysis of security- and privacy-related information; and Reporting the security and privacy status of the organization and organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]. <p>Supplemental Guidance:</p> <p>Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security and privacy to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess security and privacy controls and associated risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed.</p> <p>Continuous monitoring programs also allow organizations to maintain the authorizations of</p>	<p>L M H</p> <p>CNSSI</p> <p>FedRAMP</p> <p>800-82 ICS</p> <p>800-171 CUI</p>	<p>E</p>	<p>Deep Discovery Inspector provides continuous monitoring against newly discovered vulnerabilities, threat vectors and agents. The Deep Discovery Inspector detection engines deliver expanded APT and targeted attack detection including custom sandbox analysis. New discovery and correlation rules detect malicious content, communication, and behavior across every stage of an attack sequence. The Deep Discovery Inspector management console provides real-time threat visibility and analysis. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.</p> <p>Deep Discovery Inspector provides continuous monitoring support through the integration with the Trend Micro Threat Management Services Portal, which is part of the Trend Micro Threat Management Services. Threat Management Services is a network security over watch service that monitors global threats and other specialized vulnerability services, such as the Critical Vulnerabilities Exposure (CVE) database. The Threat Management Services integrates into an organizations existing security infrastructure and is powered by the Trend Micro Smart Protection Network.</p> <p>The Deep Discovery Inspector dashboard displays the following information on customizable and user-selected widgets: System data and status; Threat data and analysis; and Summary graphs. The dashboard also monitors real-time network traffic volumes scanned by Deep Discovery Inspector.</p> <p>Deep Discovery Email Inspector dashboard provides:</p> <ul style="list-style-type: none"> - Threat Monitoring, incoming suspicious messages, attack sources, affected recipients, and which messages were quarantined; - Trends, the top activity in the network, including suspicious message content and callback destinations, to understand the threat characteristics affecting the network. - System Status, overall email message processing volume during different time periods for different risk levels and the current Deep Discovery Email Inspector appliance hardware status. The dashboard graphically shows how system performance affects message delivery.; and - Virtual Analyzer performance based on processing time, queue size, and the volume
--	---	----------	---

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>systems and common controls over time in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing authorization decisions. Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Related Controls: AC-2, AC-6, AU-6, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, PE6, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-32, RA-3, RA-5, RA-7, SA-11, SC-5, SC-38, SI-3, SI-4, SI-12.</p> <p>References: NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-122, 800-137; NIST Interagency Reports 8011, 8062.</p>			<p>of suspicious objects discovered during analysis.</p> <p>Deep Discovery Analyzer supports continuous monitoring through the dashboard capability which provides:</p> <ul style="list-style-type: none"> - Summary, to understand threats detected by Deep Discovery Analyzer based on type and amount, the volume of suspicious objects discovered during analysis, - Submissions over time, and the Virtual Analyzer summary. - System Status, to understand the overall performance of Deep Discovery Analyzer based on Virtual Analyzer status, queued samples, and the hardware status. <p>Deep Security uses multiple techniques to identify suspicious behavior. The anti-malware engine identifies suspicious programs or processes. Using Integrity Monitoring or Log Inspection provides early indicators of compromise. All of these capabilities can run in real-time or can be scheduled for regular scans. In addition the Recommendation scan can help support this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits.</p> <p>Deep Security also assists in continuous monitoring by the use of dashboards. Dashboards are the primary user interface for monitoring and troubleshooting Deep Security issues. The following custom dashboards are available in the management pack:</p> <ul style="list-style-type: none"> - Deep Security Top 10 Analysis by total event count for key performance metrics (KPIs). - Deep Security Troubleshooting health information regarding Deep Security resources in a relationships view as well as KPIs for the selected Deep Security resource. - Deep Security Total Event Count Heat Map displays at-a-glance data regarding all Deep Security Manager events, using heat maps and event breakdown charts. <p>TippingPoint support continuous monitoring through the Security Management System dashboard. The SMS dashboard provides at-a-glance monitors with launch capabilities into the targeted management applications that provide global command and control of TippingPoint. Included in the SMS dashboard display are the following items:</p> <ul style="list-style-type: none"> - Entries for the top five filters triggered over the past hour in various categories - A graph of triggered filters over the past 24 hours - The health status of devices - Update versions for software of the system <p>Through the Dashboard, an overview of the current performance of the system is provided, including notifications of updates and possible issues with devices monitored by the SMS.</p>

CA-8 Security Assessment and Authorization / Penetration Testing

CA-8 Security Assessment and Authorization / Penetration Testing Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components]. Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is most effectively conducted by penetration testing agents and teams with demonstrable skills and experience that, depending on the scope of the penetration testing, include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to either validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include, for example, time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries in carrying out attacks against organizations and provides a more in-depth analysis of security- and privacy related weaknesses or deficiencies. Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes, for example, pretest analysis based on full knowledge of the target system; pretest identification of potential vulnerabilities based on pretest analysis; and testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P CNSSI FedRAMP 800-82 ICS 800-171 CUI	<p>Deep Security Recommendation Scan assists in supporting this requirement for external penetration testing of an organization external facing systems. Deep Security Recommendation Scan automates scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used in support the penetration testing effort.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC <u>Security Targets</u> include the following control which are mapped (in SP 800-53 Table I-3) to supporting the CA-8 control:</p> <ul style="list-style-type: none"> - AVA_VAN.2 (<i>Vulnerability Assessment/ Vulnerability Analysis</i>) – “The evaluator performs penetration testing ...”
--	--	--	---

commencement of penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Risk assessments guide the decisions on the level of independence required for personnel conducting penetration testing. Related Controls: SA-11, SA-12.

CM-2 Configuration Management / Baseline Configuration

<p>CM-2 (2) Configuration Management / Baseline Configuration / Automation Support for Accuracy / Currency</p> <p>Employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the system.</p> <p>Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the system level, or at the operating system or component level including, for example, on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used, for example, to track version numbers on operating systems, applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8(2) for organizations that choose to combine system component inventory and baseline configuration activities. Related Controls: CM-7, IA-3, RA-5.</p>	<p>H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E</p>	<p>Deep Discovery Analyzer, Deep Discovery Email Inspector, and Deep Discovery Inspector integrate with Deep Discovery Director which is an on-premises management solution that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication and log aggregation for Deep Discovery products. To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode..</p> <p>The Deep Security solution supports compliance with this requirement by the Integrity Monitoring, Recommendation Scans, and Application Control functionality. Integrity Monitoring ensures that critical security files are monitored for changes as part of an automated process to ensure accuracy and availability of these files. The Recommendation Scanning engine is a framework that exists within Deep Security Manager, which allows the system to suggest and automatically assign security configuration. The goal is to make configuration of hosts easier and only assign security required to protect that host. The Application Control can be used to lock down the system to ensure only approved applications are allowed to run.</p> <p>TippingPoint Security Management System (SMS) enables a remote monitor and manage IPS devices and perform the following tasks:</p> <ul style="list-style-type: none"> - View, manage and edit device configuration. - Review logs and reports. - Configure virtual ports and security policy. - Distribute the port and policy configuration to multiple IPS devices. - From a network management system (NMS), remote monitoring of events and system status of the IPS device. Configuring an NMS enables applications to monitor the IPS device.
<p>CM-2 (6) Configuration Management / Baseline Configuration / Development and Test Environments</p> <p>Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.</p> <p>Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments helps protect systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments. Related Controls: CM-4, SC-3, SC-7.</p>	<p>800-171 CUI</p>	<p>E</p>	<p>The Deep Security solution can assist in satisfying this requirement through the Integrity Monitoring, which compares the current condition of a monitored object with an existing baseline. Integrity Monitoring monitors critical system objects such as files, folders, registry entries, processes, services, and listening ports and can assist in developing a systems baseline configuration and notifying administrators of any modifications to it. In addition, the Application Control can be used to lock down the system to ensure only approved applications are allowed to run.</p>

CM-3 Configuration Management / Configuration Change Control

<p>CM-3 Configuration Management / Configuration Change Control</p> <ol style="list-style-type: none"> a. Determine the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time-period]; 	<p>M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>TippingPoint assists in meeting this requirement through the Common Criteria certification specifically the Life Cycle Support and the assurance requirement specified as Authorized Controls.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific</p>
--	---	----------	--

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>f. Monitor and review activities associated with configuration-controlled changes to the system; and</p> <p>g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].</p> <p>Supplemental Guidance: Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems; changes to configuration settings for component products; unscheduled or unauthorized changes; and changes to remediate vulnerabilities. Configuration change control elements can include such entities as committees or boards. Typical processes for managing configuration changes to systems include, for example, Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to organizational systems and the auditing activities required to implement such changes. Related Controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, SA-10, SA-19, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10. References: NIST Special Publications 800-124, 800-128; NIST Interagency Report 8062.</p>			<p>SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following control which are mapped (in SP 800-53 Table I-3) to supporting the CM-3 control:</p> <ul style="list-style-type: none"> - ALC_CMC.3 (Life-Cycle Support/CM Capabilities/ Use of a CM System).

CM-5 Configuration Management / Access Restrictions for Change

CM-5 (2) Configuration Management / Access Restrictions for Change / Review System Change Settings Review system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred. Supplemental Guidance: Indications that warrant review of system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. Related Controls: AU-6, AU-7, CM-3.	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Security supports compliance with this requirement through the Deep Security audit functionality and through the Integrity Monitoring functionality which can assist in determining if a modification has taken place to a critical object and alert administrators to these configuration modifications.</p> <p>TippingPoint can review IPS configuration settings through the operating system command – “show”, which displays the current status of IPS hardware and software components and a view of the information in the current configuration files. In addition, the TippingPoint SMS maintains a full change history including version control for all security policies.</p>
--	--	---	---

CM-6 Configuration Management / Configuration Settings

CM-6 Configuration Management / Configuration Settings a. Establish and document configuration settings for components employed within the system using [Assignment: organization-defined common secure configurations] that reflect the most restrictive mode consistent with operational requirements; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization defined operational requirements]; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures. Supplemental Guidance: Configuration settings are the parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers, workstations, input/output devices, network devices, operating systems, and applications. Security-related parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline.	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Security supports satisfying this requirement through the Integrity Monitoring functionality which alerts an administrator of a physical or virtualized environment of modifications to critical security configuration objects. In addition the Deep Security solution has introduced within the virtualized environment hypervisor integrity monitoring utilizing Intel TPM/TXT technology to monitor whether the hypervisor is compromised.</p> <p>The Recommendation Scanning function that exists within Deep Security Manager also supports compliance with this requirement, by creating default policies that can be automatically assigned to a new server when it comes online and allowing the system to automatically assign security configuration to existing servers. The goal is to automate configuration of hosts and assign the security policies required to protect that server/host.</p> <p>As additional information - Deep Security can run Recommendation Scans on computers to identify known vulnerabilities. The operation scans the operating system and installed applications. Based on what is detected, Deep Security will recommend security Rules that should be applied. During a Recommendation Scan, Deep Security Agents scan:</p> <ul style="list-style-type: none"> - the operating system, - installed applications, - the Windows registry, - open ports, - the directory listing, - the file system, - running processes and services, and
---	--	---	--

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Implementation of a specific common secure configuration may be mandated at the organizational or mission/business process level or may be mandated at a higher level including, for example, by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings. Related Controls: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, RA-5, SA-4, SA-5, SA-9, SC-18, SC-19, SC-28, SC-43, SI-2, SI4, SI-6. References: NIST Special Publications 800-70, 800-126, 800-128; US Government Configuration Baselines; National Checklist Repository.</p>			<ul style="list-style-type: none"> - users. <p>For large deployments, Trend Micro recommends managing Recommendations at the Policy level. That is, all computers that are to be scanned should already have a Policy assigned to them. This way, an organization can make all rule assignments from a single source (the Policy) rather than having to manage individual rules on individual computers.</p> <p>Recommendation Scans can be initiated manually or can be a Scheduled Task to periodically run scans on specified computers.</p> <p>TippingPoint as a product can review IPS configuration settings through the operating system command – “show”, which displays the current status of IPS hardware and software components and a view of the information in the current configuration files. In addition, the TippingPoint SMS maintains a full change history including version control for all security policies</p>
<p>CM-6 (1) Configuration Management / Configuration Settings / Automated Central Management / Application / Verification</p> <p>Employ automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined system components].</p> <p>Related Controls: CA-7</p>	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Security supports this requirement through the Integrity Monitoring functionality, which alerts an administrator of a physical or virtualized environment of modifications to critical security configuration objects.</p> <p>Recommendations Scans, also support this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, and to automatically apply Deep Security rules/filters to detect/prevent exploitation of the identified vulnerabilities.</p> <p>TippingPoint can assist in supporting this requirement through the Security Management System (SMS). The SMS Server is an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices.</p> <p>The SMS provides the following functionality:</p> <ul style="list-style-type: none"> - Enterprise-wide device status and behavior monitoring — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status. - IPS networking and configuration — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group. - Filter customization — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings. - Filter and software distribution — Monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS client. The SMS client and Central Management Server can distribute these packages according to segment group settings. The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates. <p>In addition, the TippingPoint SMS maintains a full change history including version control for all security policies.</p>

CM-9 Configuration Management / Configuration Management Plan

CM-9 Configuration Management / Configuration Management Plan Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management;	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Security and Deep Discovery Inspector support this control through the Common Criteria certification and specifically the evidence of use of a CM system that uniquely identifies all configuration items.</p> <p>TippingPoint supports this control through the Common Criteria certification and specifically the evidence of use of a CM system that uniquely identifies all configuration items, and whether the ability to modify these items is properly controlled.</p>
--	--	---	---

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and</p> <p>e. Protects the configuration management plan from unauthorized disclosure and modification.</p> <p>Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Such plans define processes and procedures for how configuration management is used to support system development life cycle activities. Configuration management plans are typically developed during the development and acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization with subsets of the plan implemented on a system by system basis.</p> <p>Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the system components (i.e., hardware, software, firmware, and documentation) to be configuration managed. As systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control.</p> <p>Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, SA-10, SI-12.</p> <p>References: NIST Special Publication 800-128.</p>		<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the CM-9 control:</p> <ul style="list-style-type: none"> - Deep Security & Deep Discovery Inspector: <ul style="list-style-type: none"> - ALC_CMC.2 (Life-Cycle Support/CM Capabilities/ Use of a CM System) - ALC_CMS.2 (Life-Cycle Support/ CM Scope/ Parts of the TOE CM Coverage) - TippingPoint: <ul style="list-style-type: none"> - ALC_CMC.3 (Life-Cycle Support/ CM Capabilities/ Authorized Controls) - ALC_CMS.3 (Life-Cycle Support/ CM Capabilities/ Implementation Representation CM Coverage)

CP-2 Contingency Planning / Contingency Plan

<p>CP-2 (6) Contingency Plan / Alternate Processing / Storage Site</p> <p>Plan for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.</p> <p>Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.</p>	<p>800-171 CUI</p>	<p>E</p>	<p>Deep Security can assist in meeting this requirement to support alternate processing sites through the Deep Security Manager (DSM) which can be installed in multi-node configuration for failover and protected machines (regardless of agent or agentless) can be provisioned automatically with agents using deployment scripts. The deployment scripts that can be used to script the deployment of the Deep Security Agent using various orchestration tools (Chef, Puppet, etc). Using the deployment scripts allows for easier deployment of the agent. These scripts also allow activation and assignment of policy. They help to reduce the manual intervention required and reduce the management cost when deploying the agent in a VMware environment.</p> <p>Deep Security Manager supports multiple nodes operating in parallel using a single database. Running the Manager as multiple nodes provides increased reliability, redundant availability, virtually unlimited scalability, and better performance. Each node is capable of all tasks and no node is more important than any of the others. Users can sign in to any node to carry out their tasks. The failure of any node cannot lead to any tasks not being carried out. The failure of any node cannot lead to the loss of any data.</p> <p>Deep Security also supports satisfying this requirement, specifically in the virtual environment, through the ability of Deep Security policies, rules and filters, which are linked with Virtual Machines as they are moved to alternate processing - storage sites, this ensures the security remains intact after the VM move. The Recommendation Scanning function that exists within Deep Security Manager also supports compliance with this requirement, by creating default policies that can be automatically assigned to a new server when it comes online and allowing the system to automatically assign security configuration to existing servers. The goal is to automate configuration of hosts and assign the security policies(rules) required to protect that server/host .</p> <p>Deep Discovery Inspector, Deep Discovery Email Inspector and Deep Discovery Analyzer can make use of Deep Discovery Director to assist in meeting this requirement for alternate processing sites. Deep Discovery Director is an on-premises management solution that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication and log aggregation for Deep Discovery products. To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode.</p>
--	--------------------	----------	--

CP-9 Contingency Planning / Information System Backup

<p>CP-9 Contingency Planning / Information System Backup</p> <p>a. Conduct backups of user-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];</p> <p>b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];</p> <p>c. Conduct backups of system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and</p> <p>d. Protect the confidentiality, integrity, and availability of backup information at storage locations.</p> <p>Supplemental Guidance: System-level information includes, for example, system-state information, operating system software, application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed to protect the integrity of system backups include, for example, digital signatures and cryptographic hashes. Protection of backup information while in transit is beyond the scope of this control. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.</p> <p>Related Controls: CP-2, CP-6, CP-10, MP-4, MP-5, SC-13, SI-4, SI-13.</p> <p>References: FIPS Publications 140-2, 186-4; NIST Special Publications 800-34, 800-130, 800-152.</p>	<p>L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p>	<p>Deep Discovery Inspector can assist in meeting this backup requirement through the Configuration settings include both Deep Discovery Inspector and network configuration settings. Back up configuration settings by exporting them to an encrypted file. If needed, import this file to restore settings.</p> <p>Deep Discovery Email Inspector can assist in meeting this requirement through back up settings to create a copy of Deep Discovery Email Inspector appliance configuration to restore the configuration in another Deep Discovery Email Inspector appliance or to revert to the backup settings at a later time. Replicate a configuration across several Deep Discovery Email Inspector appliances by restoring the same configuration file into each appliance.</p> <p>Deep Discovery Email Inspector uses the Export settings from the management console to back up the Deep Discovery Email Inspector configuration. If a system failure occurs, they can be restored by importing the configuration file that was previously backed up.</p> <p>Deep Discovery Analyzer can assist in meeting this requirement through the ability of Deep Discovery Analyzer to automatically export submission records, analysis results, and objects to a remote server. Investigation package data is periodically purged based on available storage space.</p> <p>Deep Security can assist in meeting this requirement and each organizations or tenant's data can be subject to different backup policies. This can be useful for something like tenancy being used for staging and production where the staging environment requires less stringent backups (backups are the responsibility of the administrator setting up Deep Security Manager).</p> <p>TippingPoint can partially assist in meeting this requirement as all log data can be backed up by configuring the system to offload log messages to a remote system log.</p>
<p>CP-9 (8) Contingency Planning / System Backup / Cryptographic Protection</p> <p>Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].</p> <p>Supplemental Guidance: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to system backup information in storage at primary and alternate locations. Organizations implementing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.</p> <p>Related Controls: SC-12, SC-13, SC-28.</p>	<p>M H 800-171 CUI</p>	<p>P</p>	<p>Deep Security makes use of SSL cryptography to ensure integrity and confidentiality of critical links and uses the FIPS 140-2 approved cryptographic algorithms RSA-2048 and DSA-256.</p> <p>Deep Security has obtained FIPS 140-2 certification for the Trend Micro Cryptographic Module and the Trend Micro Java Crypto Module, see:</p> <ul style="list-style-type: none"> - Trend Micro Java Crypto Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3140 - Trend Micro Cryptographic Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3125 <p>TippingPoint can assist in meeting this requirement through the use of the FIPS Mode. The Enabled FIPS mode provides:</p> <ul style="list-style-type: none"> - crypto: Only FIPS-approved cryptographic algorithms are allowed, but some FIPS 140-2 requirements are not enforced. Once enabled, this mode can be disabled. - full: Only FIPS-approved cryptographic algorithms are allowed, and all FIPS 140-2 requirements are enforced. Once enabled, this mode cannot be disabled. Only a factory reset can take the device out of this mode. <p>In addition, TippingPoint SMS backup packages can be automatically encrypted prior to export for archival and storage.</p>

IA-2 Identification and Authentication / Organizational Users

<p>IA-2 Identification and Authentication (Organizational Users)</p> <p>Uniquely identify and authenticate organizational users or processes acting on behalf of organizational users.</p> <p>Supplemental Guidance: Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12. Organizational users include employees or individuals that organizations consider having the equivalent status of employees including, for example, contractors and guest researchers. This control applies to all accesses other than accesses that are explicitly</p>	<p>L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, Deep Security, and TippingPoint uniquely identify and authenticate organizational users prior to user activities.</p> <p>Deep Discovery Inspector, Deep Security and TippingPoint have demonstrated this capability through the Common Criteria "Identification and Authentication" security functions.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized</p>
---	---	----------	--

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>Identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.</p> <p>Related Controls: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA4, MA-5, PE-2, PL-4, SA-4.</p> <p>References: FIPS Publications 140-2, 201, 202; NIST Special Publications 800-63, 800-73, 80076, 800-78, 800-79, 800-156, 800-166; NIST Interagency Reports 7539, 7676, 7817, 7849, 7870, 7874, 7966</p>			<p><i>mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the IA-2 control:</p> <ul style="list-style-type: none"> - Deep Security & Deep Discovery Inspector: <ul style="list-style-type: none"> - FIA_ATD.1 (<i>Identification and Authentication/ User Attribute Definition</i>) - FIA_UAU.1 (<i>Identification and Authentication/ User Authentication/ Timing of Authentication</i>) - FIA_UID.1 (<i>Identification and Authentication/ User Identification/ Timing of Identification</i>) - TippingPoint: <ul style="list-style-type: none"> - FIA_ATD.1 (<i>Identification and Authentication/ User Attribute Definition</i>) - FIA_UAU.2 (<i>Identification and Authentication/ User Authentication before any Action</i>) - FIA_UID.2 (<i>Identification and Authentication/ User Identification/ User Identification before any Action</i>)

IA-3 Identification and Authentication / Device to Device

<p>IA-3 Device Identification and Authentication</p> <p>Uniquely identify and authenticate [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.</p> <p>Supplemental Guidance:</p> <p>Devices requiring unique device-to-device identification and authentication are defined by type, by device, or by a combination of type and device. Organization-defined device types may include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission/business requirements. Because of the challenges of implementing this control on large scale, organizations can restrict the application of the control to a limited number (and type) of devices based on organizational need.</p> <p>Related Controls: AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p>	<p>Deep Discovery Inspector through proxy settings is uniquely identified and authenticated prior to a connection being established with the Threat Management Services Portal, Smart Protection Network, and Trend Micro Control Manager. Deep Discovery Inspector supports this control requirement through the use of TLS 1.2 to connect to other servers and services.</p> <p>Deep Discovery Email Inspector supports this control requirement through the use of TLS 1.2 connecting two hosts the Deep Discovery Email Inspector appliance and the email relay.</p> <p>Deep Security supports compliance with this requirement for device identification and authentication through the capability of TLS 1.2 which offers a higher level of security than the preceding versions of TLS, affects the following client activities that involve downloading agent and Deep Security Virtual Appliance (DSVA) packages from Deep Security Manager:</p> <ul style="list-style-type: none"> - Running a deployment script on a computer to install agent - Deploying a DSVA OVF package to VMware vCenter <p>In support of the cryptographic functions outlined Deep Security has obtained FIPS 140-2 certification for the Trend Micro Cryptographic Module and the Trend Micro Java Crypto Module, see:</p> <ul style="list-style-type: none"> - Trend Micro Java Crypto Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3140 - Trend Micro Cryptographic Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3125 <p>TippingPoint IPS devices support the use of remote authentication servers. Administrators can select between a Remote Authentication Dial In User Service (RADIUS) server and a Terminal Access Controller Access-Control System Plus (TACACS+) server for central authentication of users.</p>
---	--	------------	--

IA-5 Identification and Authentication / Authenticator Management

<p>IA-5 Identification and Authentication / Authenticator Management</p> <p>Manage system authenticators by:</p> <ol style="list-style-type: none"> a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator 	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector provides user authentication password management capability to support this control.</p> <p>Deep Discovery Email Inspector supports this control through user role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to the accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users log on to the management console using custom user accounts.</p>
--	--	----------	--

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;</p> <ul style="list-style-type: none"> e. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; f. Changing/refreshing authenticators [Assignment: organization-defined time-period by authenticator type]; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and i. Changing authenticators for group/role accounts when membership to those accounts changes. <p>Supplemental Guidance: Examples of individual authenticators include passwords, cryptographic devices, one-time password devices, and key cards. The initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include, for example, the minimum password length. Developers may ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems including, for example, passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Actions that can be taken to safeguard individual authenticators include, for example, maintaining possession of authenticators, not loaning or sharing authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.</p> <p>Related Controls: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4.</p> <p>References: FIPS Publications 140-2, 180-4, 201, 202; NIST Special Publications 800-73, 800-63, 800-76, 800-78; NIST Interagency Reports 7539, 7817, 7849, 7870, 8040.</p>		<p>Deep Discovery Analyzer supports this control through the Password Policy capability requiring strong passwords. Strong passwords usually contain a combination of both uppercase and lowercase letters, numbers, and symbols, and are at least eight characters in length. In addition when a user exceeds the number of retries allowed while entering incorrect passwords, Deep Discovery Analyzer sets the user account to inactive (locked).</p> <p>Deep Security supports this control requirement for authenticator management through user password management such as:</p> <ul style="list-style-type: none"> - Session idle timeout: Specify the period of inactivity after which a user will be required to sign in again. - Maximum session duration: Maximum length of time that a user can be signed into the Deep Security Manager before they'll be required to sign in again. - Number of incorrect sign-in attempts allowed (before lock out): The number of times an individual user (i.e. with a specific username) can attempt to sign in with an incorrect password before they are locked out. Only a user with "Can Edit User - Properties" rights can unlock a locked-out user. Note: If a user gets locked out for a particular reason (too many failed sign-in attempts, for example), and no user remains with the sufficient rights to unlock that account, please contact Trend Micro for assistance. - Number of concurrent sessions allowed per User: Maximum number of simultaneous sessions allowed per user. <p>Action when concurrent session limit is exceeded: Specifies what happens when a user reaches the maximum number of concurrent sessions.</p> <ul style="list-style-type: none"> - User password expires: Number of days that passwords are valid. You can also set passwords to never expire. - User password minimum length: The minimum number of characters required in a password. - User password requires both letters and numbers: Letters (a-z, A-Z) as well as numbers (0-9) must be used as part of the password. - User password requires both upper and lower case characters: Upper and lower case characters must be used. - User password requires non-alphanumeric characters: Passwords must include non-alphanumeric characters. <p>TippingPoint supports this control through management of username and password values for user accounts are determined by the Security Level preference setting configured on the Preferences page. Username and password requirements are the same for local users and TippingPoint OS users. There are three possible security levels available on the IPS:</p> <ul style="list-style-type: none"> - Level 0 — User names and passwords are unrestricted. - Level 1 — Names must be at least 6 characters long; passwords at least 8. - Level 2 — In addition to level 1 restrictions, passwords must contain: at least two alpha characters: at least one numeric character; and at least one non-alphanumeric character <p>The default security level preference is Maximum Security Checking.</p> <p>TippingPoint SMS supports authentication via CAC which includes certificate expiration and management controls.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC <u>Security Target</u> includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the IA-5 control:</p> <ul style="list-style-type: none"> - FIA_SOS.1 (<i>Identification and Authentication/ Specification of Secrets</i>).

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy	
IA-5 (7) Identification and Authentication / Authenticator Management / No Embedded Unencrypted Static Authenticators Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. Supplemental Guidance: Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else.	CNSSI FedRAMP 800-171 CUI	P	Deep Discovery Inspector and Deep Security authentication takes place by matching one-way hashed passwords against values previously stored in the database. This has been demonstrated by Deep Discovery Inspector and Deep Security certified by the Common Criteria Evaluation and Certification Scheme. TippingPoint supports this requirement by not using embedded clear text authenticators and enforcing the use of hashed passwords.		

IA-7 Identification and Authentication / Cryptographic Module Authentication

IA-7 Identification and Authentication / Cryptographic Module Authentication Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines for such authentication. Supplemental Guidance: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Related Controls: AC-3, IA-5, SA-4, SC-12, SC-13. References: FIPS Publication 140-2.	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P	<p>Many Executive Orders and Directives require the implementation of FIPS 140-2 qualified crypto modules.</p> <p>TippingPoint Crypto Core OpenSSL is a software library which provides FIPS 140-2 approved cryptographic algorithms and services for TippingPoint security products. TippingPoint through the FIPS 140-2 Cryptographic Module Validation Program has been awarded Certificate #2391.</p> <p>TippingPoint can assist in meeting this requirement through the use of the FIPS Mode. The Enabled FIPS mode provides:</p> <ul style="list-style-type: none">- crypto: Only FIPS-approved cryptographic algorithms are allowed, but some FIPS 140-2 requirements are not enforced. Once enabled, this mode can be disabled.- Full: Only FIPS-approved cryptographic algorithms are allowed, and all FIPS 140-2 requirements are enforced. Once enabled, this mode cannot be disabled. Only a factory reset can take the device out of this mode. <p>Deep Security makes use of SSL cryptography to ensure integrity and confidentiality of critical links and uses the cryptographic algorithms RSA-2048 and DSA-256.</p> <p>Deep Security has obtained FIPS 140-2 certification for the Trend Micro Cryptographic Module and the Trend Micro Java Crypto Module, see:</p> <ul style="list-style-type: none">- Trend Micro Java Crypto Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3140- Trend Micro Cryptographic Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3125.		
--	--	-----	--	--	--

IR-2 Incident Response / Training

IR-2 Incident Response Training Provide incident response training to system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time-period] of assuming an incident response role or responsibility; b. When required by system changes; and c. [Assignment: organization-defined frequency] thereafter. Supplemental Guidance: Incident response training is linked to assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle and remediate incidents; and finally, incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related Controls: AT-2, AT-4, AT-3, CP-3, IR-3, IR-4, IR-8, IR-9. References: NIST Special Publication 800-50.	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Security, Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, and TippingPoint support this control through online and in class training on how the product can be used in effective incident response and handling capabilities.</p>		
---	--	---	---	--	--

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
IR-2 (1) Incident Response Training / Simulated Events Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	Deep Discovery Analyzer "sandbox" can support this control through simulating security incidents, such as APT's, and train Incident Response personnel on how to handle such incidents.
IR-2 (2) Incident Response Training / Automated Training Environments Employ automated mechanisms to provide a more thorough and realistic incident response training environment.	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	Deep Discovery Inspector as an automated breach detection, malware and APT detector can be configured to support this control through the establishment of a separate incident training environment.

IR-3 Incident Response / Testing

IR-3 Incident Response Testing Test the incident response capability for the system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results. Supplemental Guidance: Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations, organizational assets, and individuals due to incident response. Use of qualitative and quantitative data aids in determining the effectiveness of incident response processes. Related Controls: CP-3, CP-4, IR-2, IR-4, IR-8, PM-14. References: NIST Special Publications 800-84, 800-115.	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P 800-171 CUI	Deep Discovery Inspector can support this control through the implementation of the Deep Discovery Inspector Demo Toolkit, which can be used to simulate and train customers Incident Response teams in creating Incident Response policies. TippingPoint can assist in this Incident Response training requirement through the IPS which can sample a random flow of traffic and send the data to a collector server for analysis using the sFlow feature. Security teams can then get a more holistic view of traffic patterns, which enables early detection and remediation of anomalous or malicious flows. With sFlow sampling, network and security administrators establish a baseline of typical application traffic to identify unusual patterns. Users specify the following information: <ul style="list-style-type: none">- The IP address of the collection repository. Two collector IP addresses (either IPv4 or IPv6) are supported for TOS V. 3.6 and later.- The network segments that have this feature enabled. Sampling can be configured globally or on a per-segment basis.- The sample rate. This is configured at the segment level. Faster links enable larger sample rates. The data that is sampled is sent as an sFlow datagram packet to the collector server where analysis occurs. Reports can then be generated, including comparison charts that provide visibility of network congestion and potential security incidents, thereby enhancing the scalability of the network.
IR-3 (1) Incident Response Testing / Automated Testing Employ automated mechanisms to more thoroughly and effectively test the incident response capability. Supplemental Guidance: Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities. This can be accomplished, for example, by providing more complete coverage of incident response issues; by selecting more realistic test scenarios and test environments; and by stressing the response capability.			

IR-4 Incident Response / Incident Handling

IR-4 Incident Handling a. Implement an incident handling capability for security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with contingency planning activities; c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization. Supplemental Guidance: Organizations recognize that incident response capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, system owners, authorizing officials, human resources offices, physical and	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	Deep Discovery Inspector , Deep Discovery Email Inspector, Deep Discovery Analyzer, Deep Security, and TippingPoint prime functions are to detect and where possible mitigate threats and disseminate threat/attack/incident data to other systems. These products at their core consider incident response as part of their definition, design, and development. Deep Discovery Inspector can support this control by providing streamlined report and log event format for maximum efficacy when investigating complex incidents. In addition Deep Discovery Inspector can through the correlated Incident capability provide events/detections that occur in a sequence or reach a threshold and define a pattern of activity. The Deep Discovery Inspector management console provides real-time threat visibility and analysis. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures. Deep Discovery Email Inspector provides real-time threat visibility and analysis in an intuitive, multi-level format. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures. Deep Discovery Virtual Analyzer conducts incident handling through capabilities, which includes the following: <ul style="list-style-type: none">- Threat execution and evaluation summary;- In-depth tracking of malware actions and system impact; Discovery of network
--	--	---	---

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).</p> <p>Related Controls: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-8, PE-6, PL-2, PM-12, SA-12, SC-5, SC-7, SI-3, SI-4, SI-7.</p> <p>References: NIST Special Publications 800-61, 800-101, 800-86; NIST Interagency Report 7599.</p>		<p>connections initiated;</p> <ul style="list-style-type: none"> - Indications provided of system file/Registry modification; System injection behavior detection; - Identification of malicious destinations and command-and-control (C&C) servers; Exportable forensic reports and PCAP files; and - Generation of complete malware intelligence for immediate local protection. <p>Deep Security raises alerts when incidents occur that require special attention. Alerts can be raised due to security events such as the detection of malware or an abnormal restart on a protected computer, or they can be system events like the Deep Security Manager running low on disk space. Deep Security can be configured to send email notifications when specific Alerts are raised. The Log Inspection module captures and analyzes system logs to provide audit evidence for PCI DSS or internal requirements that your organization may have. It helps to identify important security events (incidents) that may be buried in multiple log entries.</p> <p>TippingPoint through Event monitoring can support this control for incident handling. Events: logs, traffic streams, reports.</p> <p>Events monitor system performance and review traffic-related events. The events review capability provides the following options:</p> <ul style="list-style-type: none"> - Logs — View information on system events and traffic-related events triggered by IPS filters and policies. Logs include alert, quarantine, block, audit, and system logs. - Managed Streams — Review and manage traffic streams that have been blocked, rate-limited, trusted, or quarantined by IPS policies. You can also manually quarantine or release a quarantined IP address. - Health — Review the current status and network performance of the IPS device. Information includes memory and disk usage statistics, status of the Threat Suppression Engine and the Ethernet ports, and throughput performance. - Reports —View graphs showing information on traffic flow, traffic-related events, and statistics on triggered filters (filter matches, rate limit, traffic, DDoS, quarantine, and adaptive filter).
<p>IR-4 (1) Incident Handling / Automated Incident Handling Processes Employ automated mechanisms to support the incident handling process.</p> <p>Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems; and tools that support collection of live response data, full network packet capture, and forensic analysis.</p>	<p>M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>Deep Discovery Inspector supports this requirement by automatically detecting suspicious/malicious network traffic indicative of networks under attack or which have been breached. Deep Discovery Inspector further expands information security teams' capability in analyzing and combating targeted attacks by recording network activities near the initial detection. In addition, the investigative process is streamlined to improve the presentation of detection results in Deep Discovery Inspector.</p> <p>Deep Discovery Email Inspector provides automated real-time threat visibility and analysis in an intuitive, multi-level format. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures. Deep Discovery Email Inspector can be configured to automatically block and quarantine email messages, allow the email messages to pass to the recipient, strip suspicious file attachments, redirect suspicious links to blocking or warning pages, or tag the email message with a string to notify the recipient.</p> <p>Deep Discovery Analyzer makes use of a custom sandboxing environment that can be created within Deep Discovery Analyzer, which precisely matches target desktop software configurations — resulting in automatic handling and accurate detections producing fewer false positives.</p> <p>Deep Security Recommendation Scan supports this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits.</p> <p>Deep Security, Intrusion Detection and Prevention module supports incident handling by automatically protecting computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. It shields vulnerabilities until code fixes can be completed and identifies malicious</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>IR-4 (1) Incident Handling / Automated Incident Handling Processes</p> <p>(... Continued.)</p>		<p>software accessing the network and increases visibility into, or control over, applications accessing the network. Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets.</p> <p>TippingPoint notifications send information to the management system when traffic thresholds are crossed and logged. TippingPoint also makes use of traffic management profiles to automatically handle incidents that have triggered an event/incident. TippingPoint also uses Action Sets to determine what the IPS device does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action. The types of action that can be specified include the following:</p> <ul style="list-style-type: none"> - Actions determine where a packet is sent after it is inspected: <ul style="list-style-type: none"> - A permit action allows a packet to reach its intended destination. - A block action discards a packet. A block action can also be configured to quarantine the host and/or perform a TCP reset. - A rate limit action enables the definition of the maximum bandwidth available for the traffic stream. - A trust action allows the designated traffic to bypass all inspection; the traffic is transmitted immediately. Trust has lower latency than Permit, and using it can reduce load on the CPU and processors. - Packet Trace allows the capture of all or part of a suspicious packet for analysis. The packet trace priority and packet trace verbosity for action sets. <ul style="list-style-type: none"> - Priority sets the relative importance of the information captured. Low priority items are discarded before medium priority items if there is a resource shortage. - Verbosity determines how much of a suspicious packet will be logged for analysis. If full verbosity is chosen, the whole packet is recorded. If partial verbosity is chosen how many bytes of the packet (from 64 to 1600 bytes) of the packet trace log records. - Notification Contacts indicate the contacts to notify about the event. These contacts can be systems, individuals, or groups.
<p>IR-4 (2) Incident Handling / Dynamic Reconfiguration</p> <p>Include dynamic reconfiguration of [Assignment: organization-defined system components] as part of the incident response capability.</p> <p>Supplemental Guidance:</p> <p>Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of systems, for example, to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for achieving the reconfiguration of systems in the definition of the reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats. Related Controls: AC-2, AC-4, CM-2.</p>	<p>FedRAMP 800-171 CUI</p>	<p>Deep Discovery Inspector supports this requirement by providing indicators of compromise (IOC) information to other Trend Micro and third-party security systems such as SIEMs, firewalls and intrusion prevention systems.</p> <p>Deep Discovery Inspector allows on-demand component updates. This feature can be used during outbreaks or when updates do not arrive according to a fixed schedule. In addition a proxy server can be used for pattern, engine, and license updates.</p> <p>Deep Discovery Email Inspector acts upon email messages according to the assigned risk level and policy settings. Deep Discovery Email Inspector can be configured to block and quarantine the email message, allow the email message to pass to the recipient, strip suspicious file attachments, redirect suspicious links to blocking or warning pages, or tag the email message with a string to notify the recipient.</p> <p>Deep Discovery Analyzer performs static and dynamic analysis to identify an object's notable characteristics during analysis. Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer generates analysis reports, suspicious object lists, PCAP files, and Open IOC files that can be used in investigations.</p> <p>Deep Security supports this requirement in its support of VMware's NSX by tagging infected virtual machines allowing them to be automatically quarantined. If a large number of computers require protection an automated process of installing and activating agents can be used. The Deep Security Manager's deployment script generator to generate scripts run on computers which will install the agents and optionally perform subsequent tasks like activation and policy assignment. The scripts are also useful as a starting template to create customized scripts to execute various additional available commands.</p> <p>The Deep Security security configuration of a VM in an NSX environment can be automatically modified based on changes to the VM's NSX Security Group. The automation of security configuration is done using the NSX Security Group Change Event-Based Task.</p> <p>Deep Security can also group computers dynamically with smart folders. A smart folder is a dynamic group of computers that are defined with a saved search query.</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>IR-4 (2) Incident Handling / Dynamic Reconfiguration</p> <p>(... Continued.)</p>		<p>It finds matching computers each time a group is selected. For example, to view computers grouped by attributes such as operating system or AWS project tags, this can be done using smart folders.</p> <p>TippingPoint makes use of sFlow sampling on a random flow of network traffic. Sampling can be configured on a global (all IPS segments) or segment-by-segment basis. When sFlow is enabled, network and security administrators can establish a baseline of typical application traffic to identify unusual patterns. Data is collected and sent as an sFlow packet to a collection repository where it is analyzed.</p> <p>TippingPoint also makes use of Adaptive Filtering with Adaptive Filtering, the Threat Suppression Engine automatically manages filter behavior when the IPS device is under extreme load conditions. This feature protects against the potential adverse effects of a filter that interacts poorly with the network environment by preventing the device from entering High Availability mode.</p> <p>Adaptive filtering works by monitoring each filter to identify any suspected of causing congestion. When it identifies a filter, it manages the filter using one of the following methods, depending on how the global or filter-level Adaptive Filtering is configured:</p> <ul style="list-style-type: none"> - Automatic Mode — This setting enables the IPS device to automatically disable and generate a system message regarding the defective filter. - Manual — This setting enables the IPS device to generate a system message regarding the defective filter. However, the filter is not disabled.
<p>IR-4 (3) Incident Handling / Continuity of Operations</p> <p>Identify [Assignment: organization-defined classes of incidents] and [Assignment: organization defined actions to take in response to classes of incidents] to ensure continuation of organizational missions and business functions.</p> <p>Supplemental Guidance:</p> <p>Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, system shutdown, fall back to manual mode/alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack.</p>	<p>CNSSI FedRAMP 800-171 CUI</p>	<p>E</p> <p>Deep Discovery Inspector supports this control through the Virtual Analyzer which provides an isolated virtual environment to manage and analyze samples with no network risk. Virtual Analyzer uses system images to observe sample behavior and characteristics, and then assigns a risk level to the sample. Virtual Analyzer is built into Deep Discovery Inspector and can be enabled at any time. Deep Discovery Inspector can also connect to an external Virtual Analyzer.</p> <p>Deep Discovery Email Inspector scans an email message for known threats in the Trend Micro Smart Protection Network, it passes suspicious files and URLs to the Virtual Analyzer sandbox environment for simulation. Virtual Analyzer opens files, including password-protected archives and document files, and accesses URLs to test for exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics. After investigating email messages, Deep Discovery Email Inspector assesses the risk using multi-layered threat analysis. Deep Discovery Email Inspector calculates the risk level based on the highest risk assigned between the Deep Discovery Email Inspector email scanners and Virtual Analyzer.</p> <p>Deep Discovery Analyzer provides indications of an attack and alerts the organization to the attack. Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match the system configuration. Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics.</p> <p>Deep Security has event-based tasks (EBTs) that can be configured to perform actions when specific events with specific conditions are detected. Deep Security further supports this requirement in its support of VMware's NSX, by tagging infected virtual machines allowing them to be automatically quarantined. Deep Security actions can be associated with event-based tasks, for example by applying a Deep Security protection policy or assigning a different relay group. Deep Security also has scheduled tasks to automate various tasks.</p> <p>TippingPoint through the SMS architecture includes the Threat Management Center (TMC) — Centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation to provide a continuity of service in the event of various attacks.</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>IR-4 (4) Incident Handling / Information Correlation</p> <p>Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.</p> <p>Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.</p>	<p>H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E</p> <p>Within Trend Micro products and services Deep Discovery Inspector supports this control through the connection with Threat Connect to search thousands of reports to provide details about detected threat behavior. Threat Connect correlates suspicious objects detected in the organization's environment and threat data from the Trend Micro Smart Protection Network. By providing on-demand access to Trend Micro intelligence databases, Threat Connect enables the ability to identify and investigate potential threats to the organization's environment. Furthermore, automated correlation facilitates the immediate generation of reports containing detailed threat analyses and remediation recommendations. These reports provide the situational awareness that is required to implement more focused response and remediation activities, and improve the organization's overall security posture.</p> <p>Threat Encyclopedia most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.</p> <p>Deep Discovery Inspector, detection engines deliver expanded APT and targeted attack detection including custom sandbox analysis. New discovery and correlation rules detect malicious content, communication, and behavior across every stage of an attack sequence. In Deep Discovery Inspector, host severity is the impact on a host as determined from aggregated detections by Trend Micro products and services. Investigating beyond event security, the host severity numerical scale exposes the most vulnerable hosts and allows to prioritize and quickly respond. Host severity is based on the aggregation and correlation of the severity of the events that affect a host. If several events affect a host and have no detected connection, the host severity will be based on the highest event severity of those events. However, if the events have a detected correlation, the host severity level will increase accordingly.</p> <p>Deep Discovery Email Inspector - Viewing Detected Messages provide intelligence about the context of a spear-phishing attack by investigating a wide array of information facets. Review the email headers to quickly verify the email message origin and how it was routed. Investigate attacks trending on the network by correlating common characteristics (examples: email subjects that appear to be the Human Resource department or fake internal email addresses). Based on the detections, change the policy configuration and warn users to take preventive measures against similar attacks.</p> <p>Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, and Deep Security can be integrated with the Trend Micro Control Manager which is a software management solution that simplifies the administration of corporate antivirus and content security policies. Control Manager provides the following centrally managed features:</p> <ul style="list-style-type: none"> - Suspicious objects, user-defined lists, and exception lists - Multiple Deep Discovery Inspector system statuses - Antivirus and content security programs, regardless of the program's physical location or platform - Consolidates multiple product solution logs <p>Deep Security Total Event Count Heat Map dashboard displays at-a-glance data regarding all Deep Security Manager events, using heat maps and event breakdown charts. The Deep Security dashboard which has numerous widgets that can be added and configured to fit the individual user's requirements. Deep Security also has some pre-package reports for help with visibility and correlation of events. Deep Security can feed events to a SIEM for further analysis of events. Lastly Deep Security has a rich set of API's that allow organizations to pull data from the system in an automated way in order to gather the information they deem critical to create their own custom reports.</p> <p>TippingPoint through the SMS architecture includes the Threat Management Center (TMC) — Centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation to provide information correlation. In addition the SMS features a policy-based operational model for scalable and uniform enterprise management. It enables behavior and performance analysis with trending reports, correlation and</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
		<p>real-time graphs. Reporting includes all, specific, and top attacks and their sources and destinations, as well as all, specific, and top peers and filters for misuse and abuse (peer-to-peer piracy) attacks. Reports can be created, saved, and scheduled using report templates. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters distribution control of these filters according to segment groups for refined intrusion prevention.</p> <p>The SMS dashboard provides at-a-glance monitors with launch capabilities into the targeted management applications that provide global command and control of TippingPoint.</p>
<p>IR-4 (8) Incident Handling / Correlation with External Organizations</p> <p>Coordinate with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses.</p> <p>Supplemental Guidance: The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multi-tiered developers, can provide significant benefits. Cross-organizational coordination with respect to incident handling can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization's operations, assets, and individuals.</p> <p>Related Controls: AU-16, PM-16.</p>	<p>CNSSI FedRAMP 800-171 CUI</p>	<p>E P</p> <p>Within Trend Micro products and services Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, and Deep Security assists with this control for external organization coordination through the Threat Management Services Portal and the Smart Protection Network. The Threat Management Services Portal provides organizations with an effective way to discover, mitigate, and manage stealthy and zero-day internal threats. Threat Management Services brings together security experts and a host of solutions to provide ongoing security services. These services ensure timely and efficient responses to threats, identify security gaps that leave the network vulnerable to threats, help minimize data loss, significantly reduce damage containment costs, and simplify the maintenance of network security. Threat Management Services combines years of Trend Micro network security intelligence and in-the-cloud servers that are part of Trend Micro Smart Protection Network to identify and respond to next-generation threats.</p> <p>The product solutions support compliance with this requirement and are part of the Trend Micro Smart Protection Network, which is coordinated and correlated to respond to the continuous emergence of new threats.</p> <p>The Trend Micro Smart Protection Network supports a cross organizational perspective on incident awareness by storing the information required for security countermeasures in a cloud database. Trend Micro carries out updates and management via the cloud providing an effective incident response. Overall the Trend Micro Smart Protection Network uses a global network of threat intelligence sensors to continually update email, web, and file reputation databases in the cloud, identifying and blocking threats in real time before they reach an organization.</p> <p>TippingPoint assists with this control through the Threat Management Center (TMC) which is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation. The TMC collects threat information and creates Digital Vaccine packages that are made available on the TMC website. The packages include filters that block malicious traffic and attacks on the network</p>
<p>IR-4 (9) Incident Handling / Dynamic Response Capability</p> <p>Employ [Assignment: organization-defined dynamic response capabilities] to effectively respond to security incidents.</p> <p>Supplemental Guidance: This control enhancement addresses the timely deployment of new or replacement organizational capabilities in response to security and privacy incidents. This includes capabilities implemented at the mission and business process level and at the system level.</p>	<p>800-171 CUI</p>	<p>E</p> <p>Deep Discovery Inspector supports this requirement by automatically detecting suspicious/malicious network traffic indicative of networks under attack or which have been breached and providing indicators of compromise (IOC) information to other Trend and third-party security systems such as SIEMs, firewalls and intrusion prevention systems.</p> <p>Deep Discovery Email Inspector acts upon email messages according to the assigned risk level and policy settings. Deep Discovery Email Inspector can be configured to block and quarantine the email message, allow the email message to pass to the recipient, strip suspicious file attachments, redirect suspicious links to blocking or warning pages, or tag the email message with a string to notify the recipient.</p> <p>Deep Discovery Analyzer performs static and dynamic analysis to identify an object's notable characteristics during analysis. Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer generates analysis reports, suspicious object lists, PCAP files, and Open IOC files that can be used in investigations.</p> <p>Deep Security through Recommendation Scan supports this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
			<p>a continuous monitoring program or audits. Deep Security Anti Malware capabilities use techniques to identify and remediate malware incidents on a particular host. This includes advanced detections such as predictive machine learning and behavioral analysis. This control can quarantine, clean or delete malware files depending on the configured settings. Deep Security further supports this requirement in its support of VMware's NSX by tagging infected virtual machines allowing them to be automatically quarantined.</p> <p>TippingPoint through the SMS architecture includes the Threat Management Center (TMC) — Centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation to provide a continuity of service in the event of various attacks.</p>
IR-5 Incident Response / Monitoring			
<p>IR-5 Incident Monitoring Track and document system security and privacy incidents.</p> <p>Supplemental Guidance: Documenting system security and privacy incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics; and evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, network monitoring; incident reports; incident response teams; user complaints; audit monitoring; physical access monitoring; and user and administrator reports.</p> <p>Related Controls: AU-6, AU-7, IR-8, PE-6, PM-29, SC-5, SC-7, SI-3, SI-4, SI-7. References: NIST Special Publication 800-61.</p>	<p>L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E P</p>	<p>Deep Discovery Inspector supports this control through the Threat Management Services Portal, which receives incident logs from Deep Discovery Inspector. The Threat Management Services Portal tracks and builds intelligence about the organization's threats and incidents providing administrative and executive reports. Deep Discovery Inspector provides a list of hosts experiencing an event (threat behavior with potential security risks, known threats, or malware) for a past 1 hour, 24-hour, 7-day, or 30-day time period. Deep Discovery Inspector tags these events as security risks/threats and makes a copy of the files for assessment. There is also the ability to view Correlated Incidents, which are the number of the incidents that match the deep correlation rule.</p> <p>Deep Discovery Email Inspector tracks security incidents through Alerts which provide immediate intelligence about the state of Deep Discovery Email Inspector. Alerts are classified into three categories:</p> <ul style="list-style-type: none"> - Critical alerts are triggered by events that require immediate attention - Important alerts are triggered by events that require observation - Informational alerts are triggered by events that require limited observation (most likely benign) <p>Deep Discovery Email Inspector documents security incidents by report generation to assist in mitigating threats and optimizing system settings. Generate reports on demand or set a daily, weekly, or monthly schedule. Deep Discovery Email Inspector offers flexibility in specifying the content for each report. The reports generate in PDF format.</p> <p>Deep Discovery Analyzer tracks and documents security incidents through its Alert and Report capability.</p> <p>Deep Security, through Deep Security Manager supports this control and its ability to produce and distribute incident data and reports as required by an organization's policies and by the Trend Micro Control Manager, which can track and distribute the reporting of security incidents detected by Deep Security. The Deep Security has a dashboard with numerous widgets that can be added and configured to fit the individual users requirements. Deep Security also has some pre-package reports for help with visibility and correlation of security events. Deep Security can feed security events to a SIEM for further analysis of events. Lastly Deep Security has a set of API's that allow organizations to pull data from the system in an automated way in order to gather the information they deem critical to create their own custom reports.</p> <p>TippingPoint Local Security Manager provides a monitoring and traffic related security events capability. The Local Security Manager provides a review of Logs, Managed Streams, Health, and Reports. In addition the TippingPoint SMS Event viewer supports adding incident details and other pertinent forensic information to any/all security events via a free form text field that is also searchable.</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy			
<p>IR-5 (1) Incident Monitoring / Automated Tracking / Data Collection / Analysis</p> <p>Employ automated mechanisms to assist in the tracking of security and privacy incidents and in the collection and analysis of incident information.</p> <p>Supplemental Guidance:</p> <p>Automated mechanisms for tracking incidents and for collecting and analyzing incident information include, for example, Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.</p> <p>Related Controls: AU-7, IR-4.</p>	H CNSSI 800-82 ICS 800-171 CUI	E P	<p>Within the Trend Micro services the Smart Protection Network uses a global network of threat intelligence sensors to continually update email, web, and file reputation databases in the cloud, identifying and blocking threats in real time before they reach the organization.</p> <p>Deep Discovery Inspector automatically maintains logs about security incidents, events, and updates. Queries can be used to gather information and create reports from the log database. These logs are stored in the Deep Discovery Inspector database, and in the Trend Micro Control Manager (TMC) database, or on a Syslog server.</p> <p>Deep Discovery Email Inspector tracks security incidents through Alerts which provide immediate intelligence about the state of Deep Discovery Email Inspector. Alerts are classified into three categories:</p> <ul style="list-style-type: none"> - Critical alerts are triggered by events that require immediate attention - Important alerts are triggered by events that require observation - Informational alerts are triggered by events that require limited observation (most likely benign) <p>Deep Discovery Email Inspector documents security incidents by report generation to assist in mitigating threats and optimizing system settings. Generate reports on demand or set a daily, weekly, or monthly schedule. Deep Discovery Email Inspector offers flexibility in specifying the content for each report. The reports generate in PDF format.</p> <p>Deep Discovery Analyzer makes use of the Trend Micro Smart Protection technology a next-generation, in-the-cloud protection solution providing File and Web Reputation Services. By integrating Web Reputation Services, Deep Discovery Analyzer can obtain reputation data for websites that users attempt to access. Deep Discovery Analyzer logs URLs that Smart Protection technology verifies to be fraudulent or known sources of threats and then uploads the logs for report generation.</p> <p>Deep Security, Deep Security Manager supports this control through its ability to automatically produce and distribute incident data and reports as required by an organization's policies and by the Trend Micro Control Manager, which can track and distribute the reporting of security incidents detected by Deep Security. Deep Security has a dashboard with numerous widgets that can be added and configured to fit the individual user's requirements. Deep Security also has pre-package reports for help with visibility and correlation of events. Deep Security can feed events to a SIEM for further analysis of events. Lastly, Deep Security has a rich set of API's that allow organizations to pull data from the system in an automated way in order to gather the information they deem critical to create their own custom reports.</p> <p>TippingPoint through the SMS provides centralized administration, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices. The SMS provides the following functionality:</p> <ul style="list-style-type: none"> - <u>Enterprise-wide device status and behavior monitoring</u> — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status. - <u>IPS networking and configuration</u> — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group. - <u>Filter customization</u> — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings. - <u>Filter and software distribution</u> — Monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS client. The SMS client and Central Management Server can distribute these packages according to segment group settings. The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates. 			

IR-6 Incident Response / Reporting

<p>IR-6 (1) Incident Reporting / Automated Reporting Employ automated mechanisms to assist in the reporting of security and privacy incidents.</p>	<p>M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E</p>	<p>Deep Discovery Inspector supports this control through its ability to automatically produce and distribute alerts and detailed threat intelligence reports as required by an organization's policies. Deep Discovery Email Inspector provides reports to assist in mitigating threats and optimizing system settings. Generate reports on demand or set a daily, weekly, or monthly schedule. Deep Discovery Email Inspector offers flexibility in specifying the content for each report. The reports are generated in PDF format. Deep Discovery Analyzer tracks and documents security incidents through its Alert and Report capability. Deep Security supports this control through its ability to automatically produce and distribute alerts and reports as required by an organization's policies. Deep Security has a dashboard with numerous widgets that can be added and configured to fit the individual users requirements. Deep Security also has pre-package reports for help with visibility and correlation of events. Deep Security can feed events to a SIEM for further analysis of events. Lastly Deep Security has a rich set of API's that allow organizations to pull data from the system in an automated way in order to gather the information they deem critical to create their own custom reports. In addition, the Trend Micro Control Manager supports this requirement by automating the distribution and reporting of alerts and security incidents detected by Deep Security and Deep Discovery Inspector. TippingPoint provides a number of real time reports dealing with: <ul style="list-style-type: none"> - <u>Filter Matches</u> — Displays data on traffic that has been filtered by the device based on the Digital Vaccine filter configuration in a Security Profile. - <u>Rate Limits</u> — Displays a bar graph showing the percentage of rate-limit bandwidth used for each action set configured with a rate limit. - <u>Traffic</u> — Displays traffic flow data categorized by transmission type, protocol, frame size, and port. - <u>DDoS</u> — Displays the number of DDoS attacks on the system. - <u>Quarantine</u> — Provides data on the number of hosts that have been quarantined over a selected time period; and - <u>Adaptive Filter</u> — Displays the global Adaptive Filter settings and a list of the 10 most recent filters impacted by adaptive filtering. </p>
<p>IR-6 (2) Incident Reporting / Vulnerabilities Related to Incidents Report system vulnerabilities associated with reported security and privacy incidents to [Assignment: organization-defined personnel or roles].</p>	<p>CNSSI 800-171 CUI</p>	<p>E</p>	<p>An organization can leverage the capabilities of Deep Discovery Inspector and Deep Security to report on discovered vulnerabilities associated with security incidents to an appointed person or role within the organization. Deep Discovery Inspector through the Control Manager has an alert incident setting, which indicates a potential vulnerability attack and provides a system-wide perspective of a potential attack caused by system vulnerabilities. Vulnerability reporting is generated within Deep Security Manager, along with alert generations, and automated report creation and delivery. In addition, Deep Security supports satisfying this requirement by providing, to an organization, updates to vulnerability rules that shield known and reported vulnerabilities. Rules that shield newly discovered or reported vulnerabilities are automatically delivered, often within hours, and can be pushed-out to thousands of servers and end-user systems within minutes, without the need for disruptive system restarts. Deep Discovery Analyzer makes use of the Threat Encyclopedia to combat complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities. TippingPoint makes use of the Threat Management Center specifically the Application Protection capability which defends against known and unknown exploits that target applications and operating systems: <ul style="list-style-type: none"> - <u>Attack Protection filters</u> — Detect and block traffic known to be malicious, suspicious, and to have known security implications. These filters include vulnerabilities and exploits filters. - <u>Security Policy filters</u> — Detect and block traffic that might or might not be malicious. This traffic might be different in its format or content from standard business practice, aimed at specific software or operating systems, or contrary </p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
			<p>to a company's security policies.</p> <ul style="list-style-type: none"> - <u>Reconnaissance filters</u> — Detect and block scans, sweeps, and probes for vulnerabilities and information about your network. These filters include probes and sweeps/scans filters. - <u>Informational filters</u> — Detect and block classic Intrusion Detection System (IDS) infiltration. <p>The TippingPoint SMS supports the tracking and reporting, via the Threat Insights Portal of the SMS, of all security incidents related to each host and vulnerability imported via eVR</p>

IR-7 Incident Response / Assistance

IR-7 (1) Incident Response Assistance / Automation Support for Availability of Information / Support Employ automated mechanisms to increase the availability of incident response-related information and support. Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or the assistance capability can proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Discovery Inspector provides through the web based Management Console access to threats/incidents detected and incident report generation. Deep Discovery Inspector can also send email notifications for the following threshold based events:</p> <ul style="list-style-type: none"> - Threat Events: The number of threat events that reached the configured threshold; - High Risk Hosts Detections: Deep Discovery Inspector identified a high-risk host on your network; Suspicious Hosts Detections: The number of suspicious hosts reached the threshold; - High Network Traffic: The network traffic volume reached the threshold; File Analysis Status: Virtual Analyzer was unable to analyze files; - Virtual Analyzer Detections: Virtual Analyzer detected malicious content in a sample; Deny List: A detection matched an object in the user-defined Deny List; and - Retro Scan Detections: Retro Scan detected historical callback attempts to C&C servers in the Trend Micro global intelligence list. <p>The Trend Micro, Threat Connect service can provide incident response assistance by correlating suspicious objects detected in the organizations environment and threat data from the Trend Micro Smart Protection Network. By providing on-demand access to Trend Micro intelligence databases, Threat Connect enables an organization to identify and investigate potential threats to their environment.</p> <p>TippingPoint makes use of a web interface to SMS providing information from the Threat Management Center. The Threat Management Center is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.</p>
--	--	---	--

MA-2 Maintenance / Controlled Maintenance

MA-2 (2) Maintenance / Controlled Maintenance / Automated Maintenance Activities (a) Employ automated mechanisms to schedule, conduct, and document maintenance, repair, and replacement actions for the system or system components; and (b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed. Related Controls: MA-3.	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Security has many maintenance tasks that can be performed automatically on a regular basis. Scheduled tasks are useful when deploying Deep Security in an environment and also later, to keep the system up to date and functioning smoothly. They are especially useful for running scans on a regular basis during off-peak hours. Deep Security also allows for automated upgrade of the Deep Security agent via the Deep Security Manager console to allow security administrators to ensure the latest agents are always running on a particular host.</p> <p>Deep Discovery Inspector and Deep Discovery Email Inspector can download and deploy product components used to scan for and detect network threats. Trend Micro frequently creates new component versions, perform regular updates to address the latest threats.</p> <p>Deep Discovery Analyzer Active Update provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.</p> <p>TippingPoint maintenance updates makes use of System Snapshots. Snapshots can create, manage, restore and import local snapshots for IPS devices. System snapshots can be restored on the same software version on which they were created. After restoring a snapshot, the device restarts.</p>
--	--	---	--

MP-5 Media Protection / Media Transport

<p>MP-5 Media Protection / Media Transport</p> <p>a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards];</p> <p>b. Maintain accountability for system media during transport outside of controlled areas;</p> <p>c. Document activities associated with the transport of system media; and</p> <p>d. Restrict the activities associated with the transport of system media to authorized personnel.</p> <p>Supplemental Guidance: System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, microfilm and paper. Controlled areas are areas or spaces for which organizations provide sufficient physical or procedural safeguards to meet requirements established for protecting information and systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization. Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related Controls: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-13, SC-28, SC-34. References: FIPS Publication 199; NIST Special Publication 800-60-1, 800-60-2.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the MP-5 control:</p> <ul style="list-style-type: none"> - ALC_DEL.1 (<i>Life-Cycle Support/ Delivery</i>).
---	--	---	---

PL-9 Planning / Central Management

<p>PL-9 Planning / Central Management</p> <p>Centrally manage [Assignment: organization-defined security and privacy controls and related processes].</p> <p>Supplemental Guidance: Central management refers to the organization-wide management and implementation of selected security and privacy controls and related processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of security and privacy controls is generally associated with the concept of common controls, such management promotes and facilitates standardization of control implementations and management and judicious use of organizational resources. Centrally-managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring. As part of the security and privacy control selection processes, organizations determine which controls may be suitable for central management based on organizational resources and capabilities. It is not always possible to centrally manage every aspect of a security or privacy control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. Those controls and control enhancements that are candidates for full or partial central management include, but are not limited to: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (all); CM-9 (1); CM-10; CM-11; CP-7 (all); CP-8 (all); SC43; SI-2, SI-3; SI-7; and SI-8. Related Controls: PL-8, PM-9. References: NIST Special Publication 800-37.</p>	800-171 CUI	E	<p>A number of Trend Micro products (Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, and Deep Security) can be integrated with Control Manager. The Trend Micro Control Manager is a software management solution that simplifies the administration of corporate antivirus and content security policies. Control Manager provides the following features:</p> <ul style="list-style-type: none"> - Centrally manages the following: - Suspicious objects, user-defined lists, and exception lists - Multiple system statuses - Antivirus and content security programs, regardless of the program's physical location or platform - Consolidates multiple product logs <p>Deep Security - The Deep Security Manager is the central management console for Deep Security. It provides visibility into the environment, allows for creation of security policies, provides system status and provides reporting on alerts and events occurring in the system.</p> <p>TippingPoint makes use of the Security Management Server to provide a centralized management capability. The SMS Server is an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices.</p>
---	-------------	---	--

PL-11 Planning / Baseline Tailoring

PL-11 Planning / Baseline Tailoring Tailor the selected control baseline by applying specified tailoring actions. Supplemental Guidance: The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. These actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific missions and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. The tailoring actions are described in Appendix G. Tailoring a control baseline is accomplished by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning values to control parameters; supplementing the control baseline with additional controls, as needed; and providing information for control implementation. The general tailoring actions in Appendix G can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in Appendix D in accordance with the security requirements from the Federal Information Security Modernization Act (FISMA) and the privacy requirements from the Privacy Act. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in Appendix G to specialize or customize the controls that represent the specific needs and concerns of those entities. Related Controls: PL-10, RA-2, RA-3, RA-9, SA-8, SA-12. References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-37, 800-39, 800-160.	L M H 800-171 CUI	E	Deep Security makes use of baseline configurations. The Integrity Monitoring baseline is the original secure state that an Integrity Scan's results will be compared against. Deep Security makes use of policies which allow collections of rules and configuration settings to be saved for easier assignment to multiple computers. <ul style="list-style-type: none">- New policies can be based on a recommendation scan of a computer to baseline the new policy on "an existing computer's current configuration". The following rules can be baselined -"Recommended Application Types and Intrusion Prevention Rules", "Recommended Integrity Monitoring Rules", and "Recommended Log Inspection Rules" from among the computer's properties.- Policies are intended to be created in a hierarchical structure. An administrator, can baseline policies from which to create multiple levels of child policies that get progressively more granular in their detail. Applicable rules can be assigned and other configuration settings at the top-level policies and then get more targeted and specific down through levels of child policies, eventually arriving at rule and configuration assignments at the individual computer level. The Deep Security Application Control module monitors changes — "drift" or "delta" — compared to the computer's baseline (original) software. Once application control is enabled, all software changes are logged and events are created when it detects new or changed software on the file system. When Deep Security Agent detects changes, an organization can allow or block the software, and optionally lock down the computer. TippingPoint with sFlow sampling, network and security administrators establish a baseline of typical application traffic to identify unusual patterns.
--	----------------------	---	---

PM-6 Program Management / Measures of Performance

PM-6 Program Management / Measures of Performance Develop, monitor, and report on the results of information security and privacy measures of performance. Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the security and privacy controls employed in support of the program. Related Controls: CA-7. References: NIST Special Publications 800-55, 800-137.	800-82 ICS 800-171 CUI	E	Deep Discovery Inspector, Deep Discovery Email Inspector, and Deep Discovery Analyzer monitor and report on network integrity with a dashboard. Each management console user account is provided a partially independent dashboard. Changes to a user account's dashboard affect the dashboards of other user accounts. The product dashboards can be customized with available widgets to provide timely and accurate system status and threat information about the network. Deep Discovery Inspector dashboard displays the following information on customizable and user-selected widgets: <ul style="list-style-type: none">- System data and status- Threat data and analysis- Summary graphs The dashboard also monitors real-time network traffic volumes scanned by Deep Discovery Inspector. Deep Discovery Email Inspector makes use of Advanced Threat Indicators which show the type, amount, and risk level of advanced threat indicators detected in all email messages. Deep Discovery Analyzer makes use of the investigation package which helps administrators and investigators inspect and interpret threat data generated from samples analyzed by Virtual Analyzer. It includes files in OpenIOC format that describe Indicators of Compromise (IOC) identified on the affected host or network. Deep Security Dashboards are the primary user interface for monitoring and reporting Deep Security issues. The Deep Security dashboard has numerous widgets that can be added and configured to fit the individual user's requirements. Deep Security also has pre-package reports for help with visibility and correlation of events. These reports can be automatically generated and emailed via a scheduled task. Deep Security can feed events to a SIEM for further analysis of events. Lastly, Deep Security has a rich set of API's that allow organization to pull data from the system in an automated way in order to gather the information they deem critical to create their own custom reports. TippingPoint SMS dashboard provides at-a-glance monitors with launch capabilities into the targeted management applications that provide global command and control of TippingPoint. Included in the SMS dashboard display are the following items:
---	---------------------------	---	---

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>PM-6 Program Management / Measures of Performance (Continued ...)</p>			<ul style="list-style-type: none"> - Entries for the top five filters triggered over the past hour in various categories - A graph of triggered filters over the past 24 hours - The health status of devices - Update versions for software of the system <p>The TippingPoint dashboard provides an overview of the current performance of the system, including notifications of updates and possible issues with devices monitored by the SMS. The TippingPoint SMS Threat Insights is an aggregation portal that takes events from TippingPoint NGIPS, vulnerability scanners, and sandboxing solutions and displays them in one place to prioritize, automate, and consolidate network threat information. This allows multiple security groups to have a common framework for evaluation and resolution. By automating the aggregation of threat data from multiple security tools, Threat Insights assists organizations by prioritizing incident response measures for breaches or potential vulnerabilities, and highlights preemptive actions already taken to protect the organizations network.</p> <p>The SMS Threat Insights portal provides real time indication of hosts that are breached and require the most attention:</p> <ul style="list-style-type: none"> - Based on the number of times a host has been breached; - Based on the number of times a threat has been detected; - What vulnerabilities exist and which Digital Vaccine (DV) filters can be applied to provide protection; - Vulnerabilities currently protected by DV filters or virtual patches and those vulnerabilities that may have a DV filter available, but not applied; - Which zero-day threats have been detected; - Determination if undisclosed zero-day DV filters fire, requiring immediate attention.

PM-16 Program Management / Threat Awareness Program

<p>PM-16 (1) Program Management / Threat Awareness Program / Automated Means for Sharing Threat Intelligence</p> <p>Utilize automated means to maximize the effectiveness of sharing threat intelligence information.</p> <p>Supplemental Guidance: To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By utilizing well established frameworks, services, and automated tools, organizations greatly improve their ability to rapidly share and feed into monitoring tools, the relevant threat detection signatures.</p>	800-171 CUI	E	<p>Trend Micro provides a number of services to Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, and Deep Security to support this control.</p> <ul style="list-style-type: none"> - <u>Smart Feedback</u> -Shares anonymous threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. Trend Micro Smart Feedback may include product information such as the product name, ID, and version, as well as detection information including file types, SHA-1 hash values, URLs, IP addresses, and domains. - <u>Threat Connect</u> - Correlates suspicious objects detected in an environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable an investigation of potential threats and take actions pertinent to the attack profile. - <u>Web Reputation Services</u> - Tracks the credibility of web domains. Web Reputation Services assigns reputation scores based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. - <u>Certified Safe Software Service (CSSS)</u> - Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources. - <u>Community File Reputation</u> - Determines the prevalence of detected files. Prevalence is a statistical concept referring to the number of times a file was detected by Trend Micro sensors at a given time. <p>TippingPoint Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.</p>
---	-------------	---	---

RA-3 Risk Assessment / Risk Assessment

<p>RA-3 Risk Assessment / Risk Assessment</p> <p>a. Conduct a risk assessment, including the likelihood and magnitude of harm, from:</p> <ol style="list-style-type: none"> 1. The unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 2. Privacy-related problems for individuals arising from the intentional processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization 	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following control which are mapped (in SP 800-53 Table I-3) to supporting the RA-3 control:</p>
---	--	---	---

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>and missions/business process perspectives with system-level risk assessments;</p> <p>c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; </p> <p>d. Review risk assessment results [Assignment: organization-defined frequency]; </p> <p>e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and </p> <p>f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.</p> <p>Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of systems. Risk assessments also take into account risk from external parties including, for example, individuals accessing organizational systems; contractors operating systems on behalf of the organization; service providers; and outsourcing entities.</p> <p>Organizations can conduct risk assessments, either formal or informal, at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, control selection, control implementation, control assessment, system authorization, and control monitoring. In addition to the information processed, stored, and transmitted by the system, risk assessments can also address any information related to the system including, for example, system design, the intended use of the system, testing results, and other supply chain-related information or artifacts. Assessments of risk can play an important role in security and privacy control selection processes, particularly during the application of tailoring guidance.</p> <p>Related Controls: CA-3, CP-6, CP-7, IA-8, MA-5, PE-3, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-32, RA-2, RA-5, RA-7, SA-9, SC-38, SI-12.</p> <p>References: NIST Special Publications 800-30, 800-39, 800-161; NIST Interagency Report 8023.</p>		<p>- AVA_VAN.2 (Vulnerability Assessment / Vulnerability Analysis / Vulnerability Analysis).</p>

RA-5 Risk Assessment / Vulnerability Scanning

<p>RA-5 Risk Assessment / Vulnerability Scanning</p> <p>a. Scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;</p> <p>b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:</p> <ol style="list-style-type: none"> 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; <p>c. Analyze vulnerability scan reports and results from control assessments;</p> <p>d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;</p> <p>e. Share information obtained from the vulnerability scanning process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and</p> <p>f. Employ vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.</p> <p>Supplemental Guidance: Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for system components, ensuring that the potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are</p>	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E</p> <p>Deep Discovery Inspector uses Host Severity levels as an impact on a host as determined from aggregated detections by Trend Micro products and services. Investigating beyond event security, the host severity numerical scale exposes the most vulnerable hosts and allows a prioritized and quick response. Deep Discovery Inspector connects to Trend Micro products and hosted services to update components by connecting to the Active Update server. Trend Micro regularly creates new component versions, and performs regular updates to address the latest threats. Deep Discovery Inspector components which are subject to manual or automatically scheduled updates are:</p> <ul style="list-style-type: none"> - Advanced Threat Scan Engine, - IntelliTrap Pattern, - IntelliTrap Exception Pattern, - Network Content Correlation Pattern, - Network Content Inspection Engine, - Network Content Inspection Pattern, - Spyware Active-monitoring Pattern, - Threat Correlation Pattern, - Threat Knowledge Base, - Virtual Analyzer Sensors, and - Virus Pattern. <p>Deep Discovery Email Inspector - the Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks. Major features include:</p> <ul style="list-style-type: none"> - Detection of zero-day threats - Detection of embedded exploit code - Detection rules for known vulnerabilities - Enhanced parsers for handling file deformities <p>Deep Discovery Analyzer - the Advanced Threat Scan Engine protects against viruses,</p>
--	--	--

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>discovered, announced, and scanning methods developed. This process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools including, for example, web-based application scanners, static analysis tools, and binary analyzers. Vulnerability scanning includes, for example, scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms. Scanning tools that facilitate interoperability include, for example, products that are Security Content Automated Protocol (SCAP) validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include, for example, the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments such as red team exercises provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).</p> <p>Related Controls: CA-2, CA-7, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-12, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7.</p> <p>References: NIST Special Publications 800-40, 800-70, 800-115, 800-126; NIST Interagency Reports 7788, 8023.</p>		<p>malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature based, behavior-based, and aggressive heuristic detection.</p> <p>Deep Security through its Recommendation Scan capability - a recommendation scan can scan protected computers, looking for vulnerable software and settings, and provide recommended security settings. The Recommendation Scan further supports this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, and to automatically update and apply Deep Security signatures, engines, patterns, and rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits.</p> <p>Deep Security also has Anti Malware capabilities that use the latest techniques to identify and remediate malware incidents on a particular host. This includes advanced detections such as predictive machine learning and behavioral analysis. This control can quarantine, clean or delete malware files depending on the configured settings.</p> <p>TippingPoint - the Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation. The TMC collects threat information and creates Digital Vaccine packages that are made available on the TMC website. The packages include filters that block malicious traffic and attacks on your network. The Reconnaissance filters — Detect and block scans, sweeps, and probes for vulnerabilities and information about an organizations network. These filters include probes and sweeps/scans filters.</p>
<p>RA-5 (2) Risk Assessment / Vulnerability Scanning / Update by Frequency / Prior to New Scan / When Identified</p> <p>Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].</p> <p>Related Controls: SI-5.</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E</p> <p>Deep Discovery Inspector through the ActiveUpdate server can be configured to check for updates to signature, patterns, and detection rules for known vulnerabilities on an organization defined frequency.</p> <p>Deep Discovery Email Inspector downloads components from the Trend Micro ActiveUpdate server, the default update source. Deep Discovery Email Inspector can be configured to download components from another update source specifically set up in the organization.</p> <p>Deep Discovery Analyzer connects to the Trend Micro hosted services, including</p> <ul style="list-style-type: none"> - Smart Protection Network, - ActiveUpdate server. ActiveUpdate provides updates for product components, including pattern files for known and new vulnerabilities. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server, and - Threat Connect. <p>Deep Security through the UpdateServer can ensure that the most up to date anti malware patterns are available on an organizations defined frequency.</p> <p>Deep Security Recommendation Scan rules/filters can be manually or automatically downloaded and applied as soon as they are made available. Trend Micro participates in software vendor vulnerability programs in order to have Deep Security signatures, engines, patterns, and rules/filters available as close to the announcement of the vulnerability as possible.</p> <p>TippingPoint Threat Management Center (TMC) makes use of Reconnaissance filters to detect and block scans, sweeps, and probes for vulnerabilities and information about an organizations network. These filters include probes and sweeps/scans filters. The SMS Threat Insights portal provides real time indication of hosts that are breached and require the most attention:</p> <ul style="list-style-type: none"> - Based on the number of times a host has been breached; - Based on the number of times a threat has been detected; - What vulnerabilities exist and which Digital Vaccine (DV) filters can be applied to provide protection; - Vulnerabilities currently protected by DV filters or virtual patches and those vulnerabilities that may have a DV filter available, but not applied; - Which zero-day threats have been detected; - Determination if undisclosed zero-day DV filters fire, requiring immediate attention.

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>RA-5 (3) Risk Assessment / Vulnerability Scanning / Breadth / Depth of Coverage Employ vulnerability scanning procedures that can identify the breadth and depth of coverage.</p> <p>Supplemental Guidance: The identification of the breadth and depth of coverage can include, for example, the system components scanned and the vulnerabilities checked.</p>	FedRAMP 800-171 CUI	<p>E</p> <p>Deep Discovery Inspector, Deep Discovery Email Inspector, and Deep Discovery Analyzer provide Depth of Coverage through dashboard displays for system data, status, data analysis and statistics, along with summary graphs, based on customizable user-selected widgets. The data displayed includes vulnerabilities scanned for and the machines checked. The dashboard also contains a real-time monitor for the amount of network traffic scanned.</p> <p>Deep Security provides vulnerability Depth of Coverage using dashboards which are the primary user interface for monitoring and reporting Deep Security issues. Deep Security dashboards have numerous widgets that can be added and configured to fit the individual user requirements. Deep Security has pre-package reports to help with visibility and correlation of events. These reports can be automatically generated and emailed via a scheduled task. Deep Security can feed events to a SIEM for further analysis of events. Lastly, Deep Security has a rich set of API's that allow organizations to pull data from the system in an automated way in order to gather the information they deem critical to create their own custom reports</p> <p>The Deep Security solution has Anti Malware capabilities that use the latest techniques to identify and remediate malware incidents on a particular host. This includes advanced detections such as predictive machine learning and behavioral analysis. This control can quarantine, clean or delete malware files depending on the configured settings.</p> <p>The Deep Security solution also supports compliance with this requirement through log inspection or audit records of the virtual or physical servers scanned and reports on the vulnerabilities checked.</p> <p>TippingPoint SMS dashboard provides Depth of Coverage and at-a-glance monitors with launch capabilities into the targeted management applications that provide global command and control of TippingPoint. Included in the SMS dashboard display are the following items:</p> <ul style="list-style-type: none"> - Entries for the top five filters triggered over the past hour in various categories; - A graph of triggered filters over the past 24 hours; - The health status of devices; - Update versions for software of the system. <p>TippingPoint through the dashboard provides an overview of the current performance of the system, including notifications of updates and possible issues with devices monitored by the SMS.</p>
<p>RA-5 (4) Risk Assessment / Vulnerability Scanning / Discoverable Information Determine unintended discoverable information about the system and take [Assignment: organization-defined corrective actions].</p> <p>Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the system to make designated information less relevant or attractive to adversaries.</p> <p>Related Controls: AU-13.</p>	CNSSI FedRAMP 800-82 ICS 800-171 CUI	<p>H</p> <p>E</p> <p>Deep Discovery Inspector, Deep Discovery Email Inspector, and Deep Discovery Analyzer can be configured with custom "sandbox" images to enable observation of files, URLs, registry entries, API calls, and other objects in environments that match the system configuration.</p> <p>Deep Security satisfies this requirement by the firewall module which will detect reconnaissance activities of intruders and provide an indication that such activity is taking place to the systems administrator.</p> <p>TippingPoint Threat Management Center (TMC) makes use of reconnaissance filters to detect and block scans, sweeps, and probes for vulnerabilities and information about an organization's network. These filters include probes and sweeps/scans filters.</p> <p>TippingPoint SMS eVR supports the import of vulnerability scan results which can then be used to automatically enable the appropriate filters providing protection and/or alerting of each attempt to exploit the vulnerabilities. SMS Threat Insights also provides an instant report of any exploit attempts targeted at each vulnerability.</p>
<p>RA-5 (6) Risk Assessment / Vulnerability Scanning / Automated Trend Analyses Employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.</p>	FedRAMP 800-171 CUI	<p>E</p> <p>Deep Discovery Inspector can automatically schedule the generation of Host Severity Reports, which provide information about threat detections by host. These threats are mapped to threat life cycle rules to determine overall host vulnerability levels, and then displayed in summary and detailed sub-reports.</p> <p>Deep Discovery Email Inspector provides a trend analysis capability to understand the top activity in the network, including suspicious message content and callback destinations, to understand the threat characteristics affecting the network</p> <p>Deep Security solution supports and provides statistical and trending information on vulnerabilities at various levels, including raw network packet data, malware and anti-virus signature file updates and effectiveness, this information can be</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
RA-5 (6) Risk Assessment / Vulnerability Scanning / Automated Trend Analyses (Continued ...)		<p>used to determine the efficiency of the mechanisms in place to counter threats. Deep Security can feed events to a SIEM for further analysis of events.</p> <p>The Deep Security, Recommendation Scan, Policies and Rules can be updated to reflect new software being installed on a computer, new operating system vulnerabilities being discovered or because a previous vulnerability was corrected by an operating system or software service pack. Because of the dynamic nature of the security requirements on a computer, the Recommendation Scans can be run on a regular/automated basis as a scheduled task, which will assess the current state of the computer and compare it against the latest Deep Security protection module updates to see if the current security Policy needs to be updated. In addition Deep Security can be configured to automatically assign and unassign Rules after a Recommendation Scan.</p> <p>TippingPoint SMS client enables behavior and performance analysis with trending reports, correlation and real-time graphs. Reporting includes all, specific, and top attacks and their sources and destinations, as well as all, specific, and top peers and filters for misuse and abuse (peer-to-peer piracy) attacks. Create, save, and schedule reports using report templates. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. It is possible to modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention.</p>
RA-5 (8) Risk Assessment / Vulnerability Scanning / Review Historic Audit Logs Review historic audit logs to determine if a vulnerability identified in the system has been previously exploited. Related Controls: AU-6, AU-11.	FedRAMP 800-171 CUI	<p>Deep Security supports compliance with this requirement by providing the audit and log information on when vulnerabilities are identified. In addition, when a new vulnerability is identified Deep Security provides updated rules, patterns and signature files to detect and block against the newly discovered vulnerability automatically. Deep Security Log Inspection module captures and analyzes system logs to provide audit evidence for control requirements. It helps to identify important security events that may be buried in multiple log entries.</p> <p>The Trend Micro Control Manager can correlate the output from Deep Security with other Trend Micro products including Deep Discovery Inspector to determine the presence of multi-vulnerability / multi-hop attack vectors.</p> <p>TippingPoint SMS Client reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. It is possible to modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention.</p>
RA-5 (10) Risk Assessment / Vulnerability Scanning / Correlate Scanning Information Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.	CNSSI FedRAMP 800-171 CUI	<p>Deep Discovery Inspector correlates and displays a list of hosts that have experienced an event in a user-defined time period. Detections are displayed from global intelligence, user-defined lists, and other sources.</p> <p>Deep Discovery Inspector makes use of Retro Scan which is a cloud-based service that scans historical web access logs for callback attempts to C&C servers and other related activities in the network. Web access logs may include undetected and unblocked connections to C&C servers that have only recently been discovered. Examination of such logs is an important part of forensic investigations to determine if the network is affected by attacks</p> <p>Deep Discovery Email Inspector assesses and correlates email message risk using multi-layered threat analysis. Upon receiving an email message, Deep Discovery Email Inspector email scanners check the email message for known threats in the Trend Micro Smart Protection Network and Trend Micro Advanced Threat Scanning Engine. If the email message has unknown or suspicious characteristics, the email scanners send file attachments and embedded URLs to Virtual Analyzer for further analysis.</p> <p>Deep Discovery Analyzer correlates through the custom sandboxing environments precisely match target desktop software configurations — resulting in more accurate detections and fewer false positives.</p> <p>The Trend Micro Control Manager can correlate the output from Deep Security with other Trend Micro products including Deep Discovery Inspector to determine the presence of multi-vulnerability / multi-hop attack vectors.</p> <p>Deep Security provides a dashboard view on multiple suspicious activities, through network packet inspection, log inspection, object integrity monitoring and audit records that could lead to a successful attack on the information system if allowed to develop. Deep Security can feed events to a SIEM for further analysis</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
		<p>of events. The Deep Security Manager collects Firewall, Intrusion Prevention, Anti-malware, Integrity Monitoring, Log Inspection and Web Reputation event logs from the Deep Security agents and appliances at every heartbeat. Once collected by the Deep Security Manager, event logs are kept for a period of time which can be configured. The default setting is one week. Event logging can be configured for event logging of individual rules as required. Event tagging can help sort events. Tags can be manually applied to events or automatically tagged. The auto-tagging feature can be used to group and label multiple events.</p> <p>TippingPoint enables behavior and performance analysis with trending reports, correlation and real-time graphs. Reporting includes all, specific, and top attacks and their sources and destinations, as well as all, specific, and top peers and filters for misuse and abuse (peer-to-peer piracy) attacks. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. It is possible to modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention.</p>

SA-3 System and Services Acquisition / System Development Life Cycle

<p>SA-3 System and Services Acquisition / System Development Life Cycle</p> <ul style="list-style-type: none"> a. Manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities. <p>Supplemental Guidance:</p> <p>A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. To apply the required security and privacy controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical missions and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel including, for example, chief information security officers, security architects, security engineers, system security officers, and chief privacy officers in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. It is also important that developers include individuals on the development team that possess the requisite security and privacy expertise and skills to ensure that the needed security and privacy capabilities are effectively integrated into the system. Role-based security and privacy training programs can ensure that individuals having key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security and privacy requirements into enterprise architecture also ensures that important security and privacy considerations are addressed early in the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with risk management strategy of the organization. Because the development life cycle of a system involves multiple organizations, including, for example, external suppliers, developers, integrators, and service providers, it is important to recognize that acquisition and supply chain risk management functions and controls play a significant role in the overall effective management of the system during that life cycle. Related Controls: AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-12, SA-15, SA-17, SA-18, SA-22.</p> <p>References: NIST Special Publications 800-30, 800-37, 800-64.</p>	<p>L M H CNSSI FedRAMP 800-82 ICS</p>	<p>P</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following control which are mapped (in SP 800-53 Table I-3) to supporting the SA-3 control:</p> <ul style="list-style-type: none"> - ALC_DVS.1 (Life-Cycle Support/ Development Security/ Identification of Security Measures). - ALC_LCD.1 (Life-Cycle Support/ Developer Defined Life-Cycle Model)
--	---	---

SA-4 System and Services Acquisition / Acquisition Process

<p>SA-4 System and Services Acquisition / Acquisition Process</p> <p>Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service:</p> <ol style="list-style-type: none"> Security and privacy functional requirements; Strength of mechanism requirements; Security and privacy assurance requirements; Security and privacy documentation requirements; Requirements for protecting security and privacy documentation; Description of the system development environment and environment in which the system is intended to operate; Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and Acceptance criteria. <p>Supplemental Guidance: System components are discrete, identifiable information technology assets including, for example, hardware, software, or firmware. These components represent the building blocks of a system. System components typically consist of commercial information technology products. Security and privacy functional requirements include security and privacy capabilities, functions and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Security and privacy assurance requirements include development processes, procedures, practices, and methodologies; and the evidence from development and assessment activities providing grounds for confidence that the required security and privacy functionality is implemented and possesses the required strength of mechanism. Security and privacy documentation requirements address all phases of the system development life cycle.</p> <p>Security and privacy requirements are expressed in terms of security and privacy controls and control enhancements that have been selected through the tailoring process. The tailoring process includes, for example, the specification of parameter values using assignment and selection statements and platform dependencies and implementation information. Security and privacy documentation provides user and administrator guidance regarding the implementation and operation of security and privacy controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the stated security or privacy capabilities, functions, or mechanisms to meet overall risk response expectations. Security and privacy requirements can include mandated configuration settings specifying allowed functions, ports, protocols, and services.</p> <p>Acceptance criteria for systems, system components, and system services are defined in the same manner as such criteria for any organizational acquisition or procurement.</p> <p>Related Controls: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12, SA-15, SA-16, SA-17, SA-21.</p>	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS</p>	<p>P</p>	<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-4 control:</p> <ul style="list-style-type: none"> - ASE_INT.1 (Security Target Evaluation/ ST introduction) - ASE_OBJ.2 (Security Target Evaluation/ Security Objectives) - ASE_REQ.2 (Security Target Evaluation/ Security Requirements/ Derived Security Requirements) - ASE_SPD.1 (Security Target Evaluation/ Security Problem Definition)
<p>SA-4 (1) Acquisition Process / Functional Properties of Security Controls</p> <p>Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.</p> <p>Supplemental Guidance: Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.</p> <p>SA-4 (2) Acquisition Process / Design / Implementation Information for Security Controls</p> <p>Require the developer of the system, system component, or system service to provide design and implementation information for the selected controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].</p> <p>Supplemental Guidance: Organizations may require different levels of detail in design and implementation documentation for controls implemented in organizational systems, system components,</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>The Common Criteria, Security Targets of Deep Discovery Inspector Deep Security, and TippingPoint provide descriptions of the functional properties of the security controls employed. Deep Discovery Inspector and Deep Security are EAL2 certified by the Common Criteria Evaluation and Certification Scheme; TippingPoint is EAL3 Augmented;</p> <p>The EAL 2/3 level provides assurance by a full Security Target (ST) and an analysis of the Security Functional Requirements and Security Assurance Requirements in that ST. The evaluation includes demonstrating adequacy of:</p> <ul style="list-style-type: none"> - functional and complete interface specification; - guidance documentation; - description of the basic modular design of Deep Discovery Inspector and Deep Security, and a subset of the implementation, to understand the security behavior; and - Product Development and Life Cycle Support capabilities. <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>or system services based on mission and business requirements; requirements for trustworthiness and resiliency; and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation may include information such as manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.</p> <p>SA-4 (3) Acquisition Process / Development Methods / Techniques / Practices Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes [Assignment: organization-defined systems engineering methods; [Selection (one or more): systems security engineering methods; privacy engineering methods]; software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].</p> <p>Supplemental Guidance: Following a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes helps to reduce the number and severity of latent errors within systems, system components, and system services. Reducing the number and severity of such errors reduces the number of vulnerabilities in those systems, components, and services.</p>	CNSSI 800-171 CUI		<p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-4 (1) and SA-4 (2) controls:</p> <ul style="list-style-type: none"> - Deep Security & Deep Discovery Inspector: <ul style="list-style-type: none"> - ADV_FSP.2 (Development/ Functional Specification/ Security-enforcing Functional Specifications) – SA-4(1) & SA4(2); - ADV_TDS.1 (Development/ TOE Design/ Basic Design) – SA-4(2); - TippingPoint: <ul style="list-style-type: none"> - ADV_FSP.3 (Development/ Functional Specifications with Complete Summary) – SA 4(1) & SA-4 (2); - ADV_TSS.1 (Security Target Evaluation/ TOE Summary Specification) – SA -4(1); - ADV_TDS.2 (Development/ TOE Design/ Basic Design)- SA-4(2)
<p>SA-4 (6) Acquisition Process / Use of Information Assurance Products</p> <p>(a) Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and</p> <p>(b) Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.</p> <p>Supplemental Guidance: Commercial off-the-shelf IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management.</p> <p>Related Controls: SC-8, SC-12, SC-13.</p>	800-171 CUI	P	<p>Deep Discovery Inspector and Deep Security are EAL2 certified by the Common Criteria Evaluation and Certification Scheme; TippingPoint is EAL3 Augmented.</p> <p>Deep Security has obtained FIPS 140-2 certification for the Trend Micro Cryptographic Module and the Trend Micro Java Crypto Module, see:</p> <ul style="list-style-type: none"> - Trend Micro Java Crypto Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3140 - Trend Micro Cryptographic Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3125 <p>TippingPoint is FIPS 140-2 Certified (certification # 2391)</p>
<p>SA-4 (7) Acquisition Process / NIAP-Approved Protection Profiles</p> <p>(a) Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance Partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and</p> <p>(b) Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated or NSA-approved.</p> <p>Related Controls: IA-7, SC-12, SC-13.</p>	CNSSI 800-171 CUI	P	<p>Deep Discovery Inspector Security Target claims demonstrable conformance to U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments, Version 1.7, July 25, 2007.</p> <p>Deep Security, Security Target and the extended Security Functional Requirement claims are based on the Intrusion Detection System (Extended Requirements) class (IDS) from the U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments. Version 1.7, July 25, 2007.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-4 control:</p> <ul style="list-style-type: none"> - ASE_CCL.1 (Security Target Evaluation/ Conformance Claims)
<p>SA-4 (8) System and Services Acquisition / Acquisition Process / Continuous Monitoring Plan for Controls</p> <p>Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of security and privacy control effectiveness that contains the following: [Assignment: organization-defined level of detail].</p>	FedRAMP 800.171 CUI	P	<p>All Trend Micro security products are developed, tested and maintained in accordance with system development and life cycle (SDLC) requirements documented in the proprietary Trend Micro Engineering Handbook (EHB).</p> <p>The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>Supplemental Guidance: The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security and privacy controls within the system, system component, or system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations.</p> <p>Related Controls: CA-7.</p>			<p>security products are now subject to the proprietary Trend Micro SDLC requirements.</p> <p>The EHB “Software Maintenance” chapter and “Engineering Tools and Services” chapter summarize details of system developer engineering processes which assist in demonstrating compliance to SA-4 (8).</p>
<p>SA-4 (9) System and Services Acquisition / Acquisition Process / Functions, Ports, Protocols, and Services in Use</p> <p>Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.</p> <p>Supplemental Guidance: The identification of functions, ports, protocols, and services early in the system development life cycle, for example, during the initial requirements definition and design phases, allows organizations to influence the design of the system, system component, or system service. This early involvement in the system life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or when requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services with organizations identifying which functions, ports, protocols, and services are provided from external sources.</p> <p>Related Controls: CM-7, SA-9.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P	Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, Deep Security, and TippingPoint provide a complete list of ports, protocols, and services within the respective products Administration Manual

SA-5 System and Services Acquisition / Information System Documentation

<p>SA-5 System and Services Acquisition / Information System Documentation</p> <p>a. Obtain administrator documentation for the system, system component, or system service that describes:</p> <ol style="list-style-type: none"> Secure configuration, installation, and operation of the system, component, or service; Effective use and maintenance of security and privacy functions and mechanisms; and Known vulnerabilities regarding configuration and use of administrative or privileged functions; <p>b. Obtain user documentation for the system, system component, or system service that describes:</p> <ol style="list-style-type: none"> User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and User responsibilities in maintaining the security of the system, component, or service and privacy of individuals; <p>c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response;</p> <p>d. Protect documentation as required, in accordance with the organizational risk management strategy; and</p> <p>e. Distribute documentation to [Assignment: organization-defined personnel or roles].</p> <p>Supplemental Guidance: This control helps organizational personnel understand the implementation and operation of security and privacy controls associated with systems, system components, and system services. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used, for example, to support the management of supply chain risk, incident response, and other functions. Personnel or roles requiring documentation may include, for example, system owners, system security officers, and system administrators. Attempts to obtain documentation may include, for example, directly contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain needed documentation may occur, for example, due to the age of the system or component or lack of support from developers and contractors. In those situations, organizations may need to recreate</p>	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Discovery Inspector, Deep Security, and TippingPoint solutions support compliance with this requirement by delivering a complete set of documentation, including but not limited to:</p> <ul style="list-style-type: none"> - Administration Manuals; - Users Guides; - Best Practices Guidelines; - Installation Manuals; and - Preparative Procedures. <p>---</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-5 control:</p> <ul style="list-style-type: none"> - AGE_OPE.1 (<i>Guidance Documents/ Operational User Guidance</i>) - AGD_PRE.1 (<i>Guidance Documents/ Preparative Procedures</i>)
---	--	---	---

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>selected documentation if such documentation is essential to the implementation or operation of the security and privacy controls. The level of protection provided for the system, component, or service documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related Controls: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12.</p>			

SA-8 System and Services Acquisition / Security Engineering Principles

<p>SA-8 System and Services Acquisition / Security Engineering Principles</p> <p>Apply [Assignment: organization-defined systems security engineering principles] in the specification, design, development, implementation, and modification of the system and system components.</p> <p>Supplemental Guidance: Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For legacy systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security and privacy engineering concepts and principles help to develop trustworthy, secure systems and system components and reduce the susceptibility of organizations to disruptions, hazards, threats, and creating privacy-related problems for individuals. Examples of these concepts and principles include, developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring security and privacy controls to meet organizational and operational needs; performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions. Security engineering principles can also be used to protect against certain supply chain risks including, for example, incorporating tamper-resistant hardware into a design.</p> <p>Related Controls: PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-12, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39.</p> <p>References: FIPS Publications 199, 200; NIST Special Publications 800-53A, 800-60-1, 800-60-2, 800-64, 800-160; NIST Interagency Report 8062.</p>	<p>M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	P	<p>Deep Discovery Inspector, Deep Security products supports compliance with this requirement by using industry best practice based system development life cycle approach. The approach is documented in the proprietary Trend Micro Engineering Handbook (EHB) as part of the Product Development Life Cycle.</p> <p>Products and modules that provide protection and security features (especially, but not limited to, those using Anti-threat protection) undergo Core Tech Certification Center certification. This is to ensure the solutions implemented by the product can (1) detect and protect against malicious attacks and (2) ensure data security. In addition a vulnerability assessment assesses the vulnerability of the product, based on established industry standards or known attacks. Test cases validate assessment reports. Test the ability to compromise the programs security. Investigate what encoding methods and user privileges can access data while transferring data on the Internet.</p> <p>The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements in the EHB.</p> <p>The EHB "Software Maintenance" and "Engineering Tools and Services" chapters summarize details of system developer engineering processes which assist in demonstrating compliance to SA-8.</p>
--	---	---	--

SA-9 System and Services Acquisition / External System Services

<p>SA-9 (2) System and Services Acquisition / External System Services / Identification of Functions, Ports, Protocols, and Services</p> <p>Require providers of [Assignment: organization-defined external system services] to identify the functions, ports, protocols, and other services required for the use of such services.</p> <p>Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.</p> <p>Related Controls: CM-6, CM-7.</p>	<p>M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	P	<p>Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, Deep Security, and TippingPoint provide a complete list of ports, protocols, and services within the respective products Administration Manual.</p>
--	---	---	---

SA-10 System and Services Acquisition / Developer Configuration Management

<p>SA-10 System and Services Acquisition / Developer Configuration Management</p> <p>Require the developer of the system, system component, or system service to:</p> <ol style="list-style-type: none"> Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; Implement only organization-approved changes to the system, component, or service; 	<p>M H CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	P	<p>Deep Discovery Inspector, Deep Security, and TippingPoint demonstrate the quality and completeness of configuration management activities as documented in the Common Criteria, Security Targets</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such</p>
---	---	---	--

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and</p> <p>e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].</p> <p>Supplemental Guidance: Organizations consider the quality and completeness of the configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include, for example, protecting from unauthorized modification or destruction, the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes. The configuration items that are placed under configuration management include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the system life cycle. Related Controls: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-12, SI-2. Refs: FIPS Pubs 140-2, 180-4, 202; NIST Special Publication 800-128.</p>		<p>mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC <u>Security Targets</u> include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-10 control:</p> <ul style="list-style-type: none"> - ALC_CMC.2 (Life-Cycle Support/ CM Capabilities/ Use of a CM System) – Deep Security & Deep Discovery Inspector; - ALC_CMC.3 (Life-Cycle Support/ CM Capabilities/ Authorization Controls) – TippingPoint; - ALC_CMS.2 (Life-Cycle) - Deep Security & Deep Discovery Inspector; - ALC_CMS.3 (Life-Cycle Support/ CM Capabilities/ Implementation Representation CM Coverage) - TippingPoint; - ALC_FLR.1 (Life-Cycle Support/ Flaw Remediation/ Basic Flaw Remediation) – Deep Security; - ALC_FLR.2 (Life-Cycle Support/ Flaw Remediation/ Flaw Reporting Procedures) – Deep Discovery Inspector & TippingPoint.
<p>SA-10 (1) System and Services Acquisition / Developer Configuration Management / Software / Firmware Integrity Verification</p> <p>Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.</p> <p>Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.</p> <p>Related Controls: SI-7.</p>	<p>CNSSI FedRAMP 800-171 CUI</p>	<p>P</p> <p>The Deep Discovery Inspector and Deep Security software can be downloaded from the Trend Micro Download web site. The product software download makes use of a SHA 256 checksum to detect if unauthorized changes to the product software have occurred.</p> <p>In addition, the Deep Discovery Inspector, Deep Security, and TippingPoint Common Criteria, Security Targets provide Delivery Procedures, which describe all procedures that are necessary to maintain security.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p>
<p>SA-10 (6) System and Services Acquisition / Developer Configuration Management / Trusted Distribution</p> <p>Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.</p> <p>Supplemental Guidance: The trusted distribution of security-relevant hardware, software, and firmware updates ensure that such updates are correct representations of the master copies maintained by the developer and have not been tampered with during distribution.</p>	<p>800-171 CUI</p>	<p>P</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC <u>Security Targets</u> include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-10 (1) and SA-10 (6) controls:</p> <ul style="list-style-type: none"> - ALC_DEL.1 (Life-Cycle Support/ Delivery)
<p>SA-10 (4) System and Services Acquisition / Developer Configuration Management / Trusted Generation</p> <p>Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.</p> <p>Supplemental Guidance: This control enhancement addresses authorized changes to hardware, software, and firmware components between versions during development. The focus is on the efficacy of the configuration management process by the developer to ensure that newly generated versions of security-relevant hardware descriptions, source code, and object code continue to enforce the security policy for the system, system component, or system service. In contrast, SA-10(1) and SA-10(3) allow organizations to detect unauthorized changes to hardware, software, and firmware components using tools, techniques, and/or mechanisms provided by developers.</p>	<p>800-171 CUI</p>	<p>P</p> <p>All Trend Micro security products are developed, tested and maintained in accordance with system development and life cycle (SDLC) requirements documented in the proprietary Trend Micro Engineering Handbook (EHB). The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements.</p> <p>The EHB “Software Maintenance” chapter and “Engineering Tools and Services” chapter summarize details of system developer engineering processes which assist in demonstrating compliance to SA-10 (4).</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>SA-10 (5) System and Services Acquisition / Developer Configuration Management / Mapping Integrity for Version Control</p> <p>Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.</p> <p>Supplemental Guidance:</p> <p>This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational systems supporting critical missions and business functions.</p>	800-171 CUI	P	<p>All Trend Micro security products are developed, tested and maintained in accordance with system development and life cycle (SDLC) requirements documented in the proprietary Trend Micro Engineering Handbook (EHB).</p> <p>The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements.</p> <p>The EHB "Software Maintenance" chapter and "Engineering Tools and Services" chapter summarize details of system developer engineering processes which assist in demonstrating compliance to SA-10 (5).</p>

SA-11 System and Services Acquisition / Developer Security Testing and Evaluation

<p>SA-11 System and Services Acquisition / Developer Security Testing and Evaluation</p> <p>Require the developer of the system, system component, or system service, at all post-design phases of the system development life cycle, to:</p> <ol style="list-style-type: none"> Create and implement a security and privacy assessment plan; Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage]; Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; Implement a verifiable flaw remediation process; and Correct flaws identified during testing and evaluation. <p>Supplemental Guidance:</p> <p>Developmental testing and evaluation confirms that the required security and privacy controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. These interconnections or changes including, for example, upgrading or replacing applications, operating systems, and firmware, may adversely affect previously implemented security and privacy controls. This control provides additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can use these analysis approaches in a variety of tools and in source code reviews. Security and privacy assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify documentation protection requirements.</p> <p>Related Controls: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-12, SA-15, SA-17, SI-2.</p> <p>References: ISO/IEC 15408; NIST Special Publications 800-30, 800-53A, 800-154.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>The Deep Discovery Inspector, Deep Security, and TippingPoint solutions support compliance with this requirement as part of the Common Criteria process independent testing of security functions, provided:</p> <ul style="list-style-type: none"> - evidence of developer testing based on the functional specification and product design, - carried out selective independent confirmation of the developer test results, - vulnerability analysis (based upon the functional specification, product design, implementation representation, security architecture description and guidance evidence provided), and - demonstrated resistance to penetration attackers with an Enhanced-Basic attack potential. <p>Deep Discovery Inspector and Deep Security are EAL2 certified by the Common Criteria Evaluation and Certification Scheme; TippingPoint is EAL3 Augmented;</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-11 control:</p> <ul style="list-style-type: none"> - ALC_FLR.1 (Life-Cycle Support/ Flaw Remediation/ Basic Flaw Remediation) – Deep Security; - ALC_FLR.2 (Life-Cycle Support/ Flaw Remediation/ Flaw Reporting Procedures) – Deep Discovery Inspector & TippingPoint; - ATE_COV.1 (Tests/ Coverage/ Evidence of Coverage) – Deep Security & Deep Discovery Inspector; - ATE_COV.2 (Tests/ Coverage/ Analysis of Coverage) - TippingPoint; - ATE_DPT.1 (Tests/ Depth/ Basic Design) – TippingPoint - ATE_FUN.1 (Tests/ Functional Testing) – Deep Security, Deep Discovery Inspector & TippingPoint.
---	--	---	---

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>SA-11 (1) System and Services Acquisition / Developer Testing and Evaluation / Static Code Analysis</p> <p>Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.</p> <p>Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews and may include, for example, checking for weaknesses in the code and checking for incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Such analysis can be used to identify vulnerabilities and enforce secure coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types; evidence that defects were inspected by developers or security professionals; and evidence that defects were remediated. An excessively high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.</p>	<p>FedRAMP 800-171 CUI</p>	<p>P</p> <p>All Trend Micro security products are developed, tested and maintained in accordance with system development and life cycle (SDLC) requirements documented in the proprietary Trend Micro Engineering Handbook (EHB). The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements.</p> <p>The EHB <i>“Product Development Lifecycle”</i>; <i>“Software Maintenance”</i> and <i>“Engineering Tools and Services”</i> chapters summarize details of system developer engineering processes which assist in demonstrating compliance to SA-11 (1) static code analysis requirements.</p>
<p>SA-11 (2) System and Services Acquisition / Developer Security Testing and Evaluation / Threat and Vulnerability Analyses</p> <p>Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses at [Assignment: organization-defined breadth and depth] during development and during the subsequent testing and evaluation of the system, component, or service that:</p> <ul style="list-style-type: none"> (a) Uses [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels]; (b) Employs [Assignment: organization-defined tools and methods]; and (c) Produces evidence that meets [Assignment: organization-defined acceptance criteria]. <p>Supplemental Guidance: Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat modeling and vulnerability analyses of those systems, system components, and system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this phase of the system development life cycle ensure that design and implementation changes have been accounted for and vulnerabilities created because of those changes have been reviewed and mitigated.</p> <p>Related controls: PM-15, RA-3, RA-5.</p>	<p>FedRAMP 800-171 CUI</p>	<p>P</p> <p>The Trend Micro Deep Discovery Inspector, Deep Security and TippingPoint family of security products support compliance with this requirement and were developed using a industry best practice based system development life cycle approach. The approach is documented in the proprietary Trend Micro Engineering Handbook as part of the Product Development Life Cycle. Products and modules that provide protection and security features (especially, but not limited to, those using Anti-threat protection) undergo Core Tech Certification Center certification. This is to ensure the solutions implemented by the product can:</p> <ul style="list-style-type: none"> - detect and protect against malicious attacks, and - ensure data security. <p>In addition a vulnerability assessment assesses the vulnerability of the product, based on established industry standards or known attacks.</p> <p>Test cases validate assessment reports. Test the ability to compromise the programs security. Investigate what encoding methods and user privileges can access data while transferring data on the Internet.</p> <p>The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements.</p> <p>----</p> <p>Deep Discovery Inspector, Deep Security are EAL2 certified by the Common Criteria Evaluation and Certification Scheme; TippingPoint is EAL3 Augmented certified by the Common Criteria Evaluation and Certification Scheme.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>“provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.”</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-11 (2) control:</p> <ul style="list-style-type: none"> - AVA_VAN.2 (<i>Vulnerability Assessment/ Vulnerability Analysis</i>).

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>SA-11 (3) System and Services Acquisition / Developer Security Testing and Evaluation / Independent Verification of Assessment Plans / Evidence</p> <p>(a) Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and</p> <p>(b) Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.</p> <p>Supplemental Guidance: Independent agents have the necessary qualifications, including the expertise, skills, training, certifications, and experience, to verify the correct implementation of developer security and privacy assessment plans.</p> <p>Related Controls: AT-3, RA-5.</p>	800-171 CUI	P	<p>Evidence of the Deep Discovery Inspector, Deep Security and TippingPoint independent testing is demonstrated through the Common Criteria process. Deep Discovery Inspector and Deep Security are EAL2 certified by the Common Criteria Evaluation and Certification Scheme; TippingPoint is EAL3 Augmented certified by the Common Criteria Evaluation and Certification Scheme.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>"provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53."</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-11 (3) control:</p> <ul style="list-style-type: none"> - ATE_IND.2 (<i>Tests/ Independent Testing/ Sample</i>).
<p>SA-11 (4) System and Services Acquisition / Developer Testing and Evaluation / Manual Code Reviews</p> <p>Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using [Assignment: organization-defined processes, procedures, and/or techniques].</p> <p>Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of systems. Such code reviews are effective in identifying weaknesses that require knowledge of the application's requirements or context which in most cases, are unavailable to automated analytic tools and techniques including static and dynamic analysis. Components benefiting from manual review include, for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls.</p>	800-171 CUI	P	<p>All Trend Micro security products are developed, tested and maintained in accordance with system development and life cycle (SDLC) requirements documented in the proprietary Trend Micro Engineering Handbook (EHB). The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements.</p> <p>The EHB <i>"Product Development Lifecycle"</i> chapter summarize details of system developer engineering processes which assist in demonstrating compliance to the SA-11 (4) manual code review requirements.</p>
<p>SA-11 (5) System and Services Acquisition / Developer Security Testing and Evaluation / Penetration Testing / Analysis</p> <p>Require the developer of the system, system component, or system service to perform penetration testing at [Assignment: organization-defined breadth and depth] and with [Assignment: organization-defined constraints].</p> <p>Supplemental Guidance: Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent implemented security and privacy features of information technology products and systems. Useful information for assessors conducting penetration testing can include, for example, product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include white-box, gray-box, or black box testing with associated analyses performed by skilled professionals simulating adversary actions. The objective of penetration testing is to uncover the potential vulnerabilities in systems, system components and services resulting from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible. Related Controls: CA-8.</p>	800-171 CUI	P	<p>Deep Discovery Inspector, Deep Security and TippingPoint satisfy this requirement by demonstrating resistance to penetration attacks with an Enhanced-Basic attack potential through the Common Criteria validation process.</p> <p>Deep Discovery Inspector and Deep Security are EAL2 certified by the Common Criteria Evaluation and Certification Scheme. TippingPoint is EAL3 Augmented certified by the Common Criteria Evaluation and Certification Scheme.</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>"provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53."</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-11 (5) control:</p> <ul style="list-style-type: none"> - AVA_VAN.2 (<i>Vulnerability Assessment/ Vulnerability Analysis</i>).

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy	
SA-11 (6) System and Services Acquisition / Developer Security Testing and Evaluation / Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews. Supplemental Guidance: Attack surfaces of systems and system components are exposed areas that make those systems more vulnerable to attacks. This includes any accessible areas where weaknesses or deficiencies in the hardware, software, and firmware components provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers analyze the design and implementation changes to systems and mitigate attack vectors generated as a result of the changes. Correction of identified flaws includes, for example, deprecation of unsafe functions.	800-171 CUI	P	<p>Trend Micro - Product Development Life Cycle, Service Engineering supports compliance with this requirement. The proprietary Trend Micro Engineering Handbook outlines the steps taken at Trend Micro to capture security vulnerabilities, track and remove security bugs. The documentation shows that all flaws are recorded and that the system tracks them to completion. It describes how Trend Micro provides user information on security flaws, corrections and guidance on corrective actions.</p> <p>The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements.</p>	
SA-11 (7) System and Services Acquisition / Developer Security Testing and Evaluation / Verify Scope of Testing / Evaluation	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of required security and privacy controls at [Assignment: organization-defined depth of testing and evaluation]. Supplemental Guidance: Verifying that testing and evaluation provides complete coverage of required security and privacy controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance corresponding to the degree of formality of the analysis. Rigorously demonstrating control coverage at the highest levels of assurance can be provided using formal modeling and analysis techniques including correlation between control implementation and corresponding test cases.	800-171 CUI	P	<p>Deep Discovery Inspector and Deep Security satisfy this requirement as evidence of security test coverage is required as part of the Common Criteria process for the products.</p> <p>Deep Discovery Inspector v3.1 has been EAL2 certified by the Common Criteria Evaluation and Certification Scheme; Deep Security v9.5 is currently being evaluated to EAL2;</p> <p>-----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-11 (7) control:</p> <ul style="list-style-type: none"> - ATE_COV.1 (Tests/ Coverage/ Evidence of Coverage) – Deep Security & Deep Discovery Inspector; - ATE_COV.2 (Tests/ Coverage/ Analysis of Coverage) - TippingPoint; - ATE_DPT.1 (Tests/ Depth/ Basic Design) – TippingPoint. 	
SA-11 (8) System and Services Acquisition / Developer Testing and Evaluation / Dynamic Code Analysis	Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis. Supplemental Guidance: Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to ensure that security functionality performs in the way it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the associated functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).	FedRAMP 800-171 CUI	P	<p>All Trend Micro security products are developed, tested and maintained in accordance with system development and life cycle (SDLC) requirements documented in the proprietary Trend Micro Engineering Handbook (EHB).</p> <p>The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements.</p> <p>The EHB “Product Development Lifecycle” chapter summarize details of system developer engineering processes which assist in demonstrating compliance to the SA-11 (8) dynamic code analysis requirements.</p>	

SA-15 System and Services Acquisition / Development Process, Standards and Tools

SA-15 System and Services Acquisition / Development Process, Standards, and Tools a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development	H CNSSI 800-82 ICS 800-171 CUI	P	<p>All Trend Micro security products are developed, tested and maintained in accordance with system development and life cycle (SDLC) requirements documented in the proprietary Trend Micro Engineering Handbook (EHB).</p> <p>The TippingPoint security products were developed by HP using proprietary and industry best practices. The ongoing support and maintenance of these acquired security products are now subject to the proprietary Trend Micro SDLC requirements.</p>
---	---	---	--

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>process; and</p> <p>4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and</p> <p>b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy [Assignment: organization-defined security and privacy requirements].</p> <p>Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes. Related Controls: MA-6, SA-3, SA-4, SA-8, SA-11, SA-12.</p>		<p>The EHB “<i>Engineering Tools and Services</i>” chapter summarize details of system developer engineering processes which assist in demonstrating compliance to the SA-11 (8) dynamic code analysis requirements.</p> <p>----</p> <p>In addition, Deep Discovery Inspector, Deep Security and TippingPoint through the Common Criteria process address this requirement through the Assurance Classes at the EAL2 level of Development, Guidance Documents, Life Cycle Support, Tests, and Vulnerability Assessment.</p> <p>Deep Discovery Inspector v3.1 has been EAL2 certified by the Common Criteria Evaluation and Certification Scheme; Deep Security v9.5 has been evaluated to EAL2. TippingPoint v 3.9 has been evaluated to EAL3 augmented.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “<i>provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.</i>” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-15 control:</p> <ul style="list-style-type: none"> - ALC LCD.1 (<i>Life-Cycle Support/ Development Security/ Developer Defined Life-Cycle Model</i>).
<p>SA-15 (6) System and Services Acquisition / Development Process, Standards, and Tools / Continuous Improvement</p> <p>Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.</p> <p>Supplemental Guidance: Developers of systems, system components, and system services consider the effectiveness and efficiency of their current development processes for meeting quality objectives and for addressing the security and privacy capabilities in current threat environments.</p>	<p>800-171 CUI</p>	<p>P</p> <p>Trend Micro is committed to support the Common Criteria process with the “evergreening” of the Deep Discovery Inspector and Deep Security products within the Common Criteria program.</p> <p>In addition, Deep Discovery Inspector, Deep Security, and Tipping Point are subjected to Continuous Improvement within the current development processes. Trend Micro releases on a regular basis product version upgrades, service packs, and patches to meet quality objectives and address security capabilities in current threat environments.</p>

SA-16 System and Services Acquisition / Developer-provided Training

<p>SA-16 System and Services Acquisition / Developer-Provided Training</p> <p>Require the developer of the system, system component, or system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms.</p> <p>Supplemental Guidance: This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of the security and privacy controls implemented within organizational systems. Training options include, for example, web-based and computer-based training; classroom-style training; and hands-on training. Organizations can also request training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.</p> <p>Related Controls: AT-2, AT-3, PE-3, SA-4, SA-5.</p>	<p>H</p> <p>CNSSI</p> <p>FedRAMP</p> <p>800-82 ICS</p> <p>800-171 CUI</p>	<p>P</p>	<p>Trend Micro satisfies this requirement by providing online and in class training on all products and services.</p>
--	---	----------	---

SA-17 System and Services Acquisition / Developer Security Architecture and Design

<p>SA-17 System and Services Acquisition / Developer Security Architecture and Design</p> <p>Require the developer of the system, system component, or system service to produce a design specification and security architecture that:</p> <ol style="list-style-type: none"> Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. <p>Supplemental Guidance: This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to ensure that organizations develop a security architecture and that the architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important when organizations outsource the development of systems, system components, or system services to external entities, and when there is a requirement to demonstrate consistency with the enterprise architecture and security architecture of the organization. ISO/IEC 15408 provides additional information on security architecture and design including, for example, formal policy models, security-relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing. Related Controls: PL-2, PL-8, PM-7, SA-3, SA-4, SA-8.</p> <p>References: ISO/IEC 15408; NIST Special Publication 800-160.</p>	<p>H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector and Deep Security address this requirement through the Common Criteria process. The Security Targets for the products provide Security Architecture and Security Design details.</p> <p>Deep Discovery Inspector v3.1 has been EAL2 certified by the Common Criteria Evaluation and Certification Scheme; Deep Security v9.5 is currently being evaluated to EAL2</p> <p>----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-17 control:</p> <ul style="list-style-type: none"> - ADV_ARC.1 (Development/ Security Architecture Description) – Deep Security, Deep Discovery Inspector & TippingPoint; - ADV_TDS.1 (Development/ TOE Design/ Basic Design) – Deep Security & Deep Discovery Inspector; - ADV_TDS.2 (Development/ TOE Design/ Architecture Design) – TippingPoint.
<p>SA-17 (4) System and Services Acquisition / Developer Security Architecture and Design / Informal Correspondence</p> <p>Require the developer of the system, system component, or system service to:</p> <ol style="list-style-type: none"> Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model; Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware. <p>Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present has no impact on the behaviors or policies being modeled. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to show such consistency. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory input and output. Related Controls: SA-5.</p>	<p>800-171 CUI</p>	<p>P</p>	<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SA-17 (4) control:</p> <ul style="list-style-type: none"> - ADV_FSP.2 (Development/ Functional Specifications/ Security-enforcing Specification) – Deep Security & Deep Discovery Inspector; - ADV_FSP.3 (Development/ Functional Specifications/ Functional Specification with Complete Summary) – TippingPoint.

SC-2 System and Communications Protection / Application Partitioning

<p>SC-2 System and Communications Protection / Application Partitioning</p> <p>Separate user functionality, including user interface services, from system management functionality.</p> <p>Supplemental Guidance:</p> <p>System management functionality includes, for example, functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is either physical or logical. Organizations implement separation of system management functions from user functions, for example, by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls.</p> <p>Related Controls: AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.</p>	<p>M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector supports the separation of systems management functionality from user functionality by the use of the Pre-Configuration Console for systems functionality and the Management Console for user functionality.</p> <p>The Pre-configuration Console is a terminal communications program that enables configuring or viewing of any pre-configuration settings, including the following:</p> <ul style="list-style-type: none"> - Network settings, and - System settings. <p>The Pre-configuration Console can be used to:</p> <ul style="list-style-type: none"> - Configure initial settings (product IP address and host name), - Roll back any updates, - Import/export device configuration, - Import HTTPS certificates, - Ping the network to verify configuration, - Perform a diagnostic test, - Restart the appliance, and - View the system logs. <p>The Management Console is used to provide and manage the user functionality. Deep Discovery Inspector provides a built-in online management console through which users can view system status, configure threat detection, configure and view logs, run reports, administer Deep Discovery Inspector, and obtain help.</p> <p>Deep Security supports compliance with this requirement by separating user functionality from systems management through the Deep Security Manager server, which is a centralized web-based management system that allows security administrators to create and manage security policies and track threats and preventive actions taken in response to them.</p>
--	--	----------	--

SC-3 System and Communications Protection / Security Function Isolation

<p>SC-3 System and Communications Protection / Security Function Isolation</p> <p>Isolate security functions from nonsecurity functions.</p> <p>Supplemental Guidance:</p> <p>The system isolates security functions from nonsecurity functions by means of an isolation boundary implemented via partitions and domains. Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Systems implement code separation in many ways, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception.</p> <p>Related Controls: AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16.</p>	<p>H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector and Deep Security through the Common Criteria process have demonstrated that the security architecture describes how the design and implementation of the product, is such, that the security features cannot be bypassed. The security domains maintained are consistent with the security functional requirements. The product is able to protect itself from tampering by untrusted active entities.</p> <p>Deep Discovery Inspector has been EAL2 certified by the Common Criteria Evaluation and Certification Scheme; Deep Security is evaluated to EAL2</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>"provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53."</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector and TippingPoint CC Security Targets include the following control which is mapped (in SP 800-53 Table I-3) to supporting the SC-3 control:</p> <ul style="list-style-type: none"> - ADV_ARC.1 (Development/ Security Architecture Design)
<p>SC-3 (2) System and Communications Protection / Security Function Isolation / Access / Flow Control Functions</p> <p>Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.</p> <p>Supplemental Guidance:</p> <p>Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include, for example, auditing, intrusion detection, and anti-virus functions.</p>	<p>800-171 CUI</p>	<p>P</p>	<p>Deep Discovery Inspector and Deep Security through the Common Criteria EAL 2 level process provide a description of the interactions among security-enforcing functions of the product, and between the security-enforcing functions of the product and other non security functions of the product.</p> <p>Deep Discovery Inspector v3.1 has been EAL2 certified by the Common Criteria Evaluation and Certification Scheme; Deep Security v9.5 is currently being evaluated to EAL2</p>

SC-5 System and Communications Protection / Denial of Service Protection

<p>SC-5 System and Communications Protection / Denial of Service Protection</p> <p>Protect against or limit the effects of the following types of denial of service events: [Assignment: organization-defined types of denial of service events or references to sources for such information] by employing [Assignment: organization-defined security safeguards].</p> <p>Supplemental Guidance: Denial of service may occur because of an attack by an adversary or a lack of internal planning to support organizational needs with respect to capacity and bandwidth. There are a variety of technologies available to limit or eliminate the effects of denial of service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by denial of service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial of service events. Related Controls: CP-2, IR-4, SC-6, SC-7, SC-40.</p>	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>The Deep Security, Firewall decreases the attack surface of the physical and virtual servers. Centralizes management of server firewall policy using a bidirectional stateful firewall. Supports virtual machine zoning and prevents denial of service attacks.</p> <p>Deep Security through TCP Packet Inspection when enabled with TCP stateful inspection will limit the number of:</p> <ul style="list-style-type: none"> - Incoming connections from a single computer to: Limiting the number of connections from a single computer can lessen the effect of a denial of service attack. - Outgoing connections to a single computer to: Limiting the number of outgoing connections to a single computer can significantly reduce the effects of Nimda-like worms. - Half-open connections from a single computer to: Setting a limit here can protect you from DoS attacks like SYN Flood. Although most servers have timeout settings for closing half-open connections, setting a value here can prevent half-open connections from becoming a significant problem. If the specified limit for SYN-SENT (remote) entries is reached, subsequent TCP packets from that specific computer will be dropped. <p>TippingPoint: The Threat Management Center, through the Infrastructure Protection filters, which protect network bandwidth and network infrastructure elements from attack, uses a combination of filter types:</p> <ul style="list-style-type: none"> - Advanced DDoS filters — Available on the 2400E and 5000E. Detect and block denial of service and flood requests, such as SYN Requests, that can overwhelm a system. - Network Equipment Protection filters — Protect networked equipment from attacks. - Traffic Normalization filters — Detect and block abnormal or malicious traffic. - The Tipping Point NGIPS protects against Distributed Denial of Service attacks.
---	--	---	---

SC-7 System and Communications Protection / Boundary Protection

<p>SC-7 System and Communications Protection / Boundary Protection</p> <p>a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system;</p> <p>b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and</p> <p>c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.</p> <p>Supplemental Guidance: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Commercial telecommunications services are typically provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Related Controls: AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PM-12, SC-5, SC-19, SC-32, SC-43. References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.</p>	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P	<p>Deep Discovery Inspector and Deep Security function as boundary protection devices. Deep Discovery Inspector can connect to the mirror port of the core switch to monitor all Internet inbound and outbound traffic from an organization, also Deep Discovery Inspector can be connected to multiple VLAN switches to monitor all ports belonging to multiple VLANs across the organization. Deep Discovery Inspector provides IT administrators with critical security information, alerts, and reports and deploys in offline monitoring mode. It monitors network traffic by connecting to the mirror port on a switch for minimal or no network interruption. Deep Discovery Inspector detects and identifies evasive threats in real-time, along with providing in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.</p> <p>Deep Security provides agentless and agent-based protection for physical, virtual, and cloud-based computers. Protection includes:</p> <ul style="list-style-type: none"> - Anti-Malware, - Web Reputation, - Firewall, - Intrusion Detection and Prevention, - Integrity Monitoring, - Application Control, and - Log Inspection. <p>Deep Security firewall solution, provides subnetwork controls that architecturally separate the public front end systems from the internal networks.</p> <p>---</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>"provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53."</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the SC-7 control:</p> <ul style="list-style-type: none"> - FDP_IFF.1 (<i>User Data Protection/ Information Flow Control Functions/ Simple</i>)
--	--	-----	---

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy
<p>SC-7 (5) System and Communications Protection / Boundary Protection / Deny by Default / Allow by Exception</p> <p>Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.</p> <p>Supplemental Guidance: This control enhancement applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections which are essential and approved are allowed. This requirement differs from CA-3(5) in that it applies to any type of network communications while CA-3(5) is applied to a system that is interconnected with another system.</p>		M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Security Attributes)</p> <p>Deep Discovery Inspector monitors all network traffic by default and can send a notification when it detects a threat that matches an object in the Deny List within the specified period. Deep Discovery Inspector allows an organization to manage the connection to entities in the Deny List.</p> <p>Deep Discovery Email Inspector through the Connection Control settings can be set to Deny all, except the following list to configure the "permit list".</p> <p>Deep Discovery Analyzer external connections are disabled by default. Trend Micro recommends enabling external connections using an environment isolated from the management network.</p> <p>Deep Security satisfies this requirement through the host firewall rules which are implemented to deny all and allow only by explicit exception.</p> <p>TippingPoint security profile defines the traffic that the IPS monitors and the DV filters that the IPS applies. Traffic monitoring is based on incoming and outgoing port pairs. The default DV filter configuration is to protect the segment or customize the configuration as required. The segment specifies both the port and the traffic direction, which allows an organization to define separate security profiles for traffic in and out of a port.</p> <p>All TippingPoint NGIPS units support the capability to limit communication to specific IP Addresses. In addition, every invalid communication attempt is both logged and reported in the System log for each NGIPS unit.</p>
<p>SC-7 (9) System and Communications Protection / Boundary Protection / Restrict Threatening Outgoing Communications Traffic</p> <p>(a) Detect and deny outgoing communications traffic posing a threat to external systems; and</p> <p>(b) Audit the identity of internal users associated with denied communications.</p> <p>Supplemental Guidance: Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out at system boundaries as part of managed interfaces. This capability includes the analysis of incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Such threats include, for example, traffic indicative of denial of service attacks and traffic containing malicious code.</p> <p>Related Controls: AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.</p>		CNSSI 800-171 CUI	E	<p>Deep Discovery Inspector can monitor and notify of outgoing malicious traffic or traffic to known malicious destinations. Deep Discovery Inspector displays all hosts with Command & Control (C&C) callbacks detected by network scanning, Deny List matches, and Virtual Analyzer detections. Viewing hosts with C&C callbacks in the past 1 hour, 24 hours, 7 days, or 30 days allows system or network administrators to take appropriate action (blocking network access, isolating computers according to IP address) in order to prevent malicious operations from affecting hosts. The detected callback type can be viewed for detailed information about the hosts and the callbacks.</p> <p>Deep Discovery Email Inspector scans an email message for known threats in the Trend Micro Smart Protection Network, it passes suspicious files and URLs to the Virtual Analyzer sandbox environment for simulation. Virtual Analyzer opens files, including password-protected archives and document files, and accesses URLs to test for exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.</p> <p>Deep Discovery Analyzer delivers full analysis results including detailed sample activities and C&C communications via central dashboards and reports.</p> <p>Deep Security supports Application Traffic rules that can provide protection in regards to outbound traffic. Rules can be defined to detect allowed protocols over unexpected ports which may be an indication of malware attempting to call home to a command and control server. The products also have the ability to detect and control unexpected protocol traffic on servers - say for example, you see FTP traffic originating from an Exchange server. Deep Security's web reputation module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of websites that users are attempting to access. The website's reputation is correlated with the specific web reputation policy enforced on the computer. Depending on the security level being enforced, Deep Security will either block or allow access to the URL.</p> <p>TippingPoint can restrict threatening outgoing communications traffic through security profiles, which define the traffic that the IPS monitors and the DV filters that the IPS applies. Traffic monitoring is based on incoming and outgoing port pairs. An organization can use the default DV filter configuration to protect the segment or customize the configuration as required. The segment specifies both the port and the traffic direction, which allows an organization to define separate security profiles for traffic in and out of a port. The default security profile is set to ANY incoming ports and ANY outgoing ports, with all IPS filters configured with the default Digital Vaccine settings. With the default profile in place, all incoming and outgoing traffic on any virtual segment configured on the device is monitored according to the IPS filter configuration recommended by TippingPoint. An organization can edit the default security profile to customize the virtual segments that it applies to and modify the filter settings, or create their own security profiles as required.</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>SC-7 (11) System and Communications Protection / Boundary Protection / Restrict Incoming Communications Traffic</p> <p>Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].</p> <p>Supplemental Guidance: This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of such address pairs in the lists of authorized/allowed communications; the absence of such address pairs in lists of unauthorized/disallowed pairs; or meeting more general rules for authorized/allowed source and destination pairs.</p> <p>Related Controls: AC-3.</p>	CNSSI 800-171 CUI	E	<p>Deep Discovery Inspector allows system or network administrators to take appropriate action (blocking network access, isolating computers according to IP address) in order to prevent malicious operations from affecting hosts.</p> <p>Deep Discovery Email Inspector prevents spear-phishing attacks and cyber threats by investigating suspicious links, file attachments, and social engineering attack patterns in email messages before they can threaten an organization's network. Designed to integrate into an organization's existing anti-spam/antivirus network topology, Deep Discovery Email Inspector can act as a mail transfer agent in the mail traffic flow (MTA mode) or as an out-of-band appliance monitoring your network for cyber threats (BCC mode or SPAN/TAP mode).</p> <p>Deep Discovery Analyzer examines suspicious objects, which are objects with the potential to expose systems to danger or loss. Deep Discovery Analyzer detects and analyzes suspicious IP addresses, host names, files, and URLs.</p> <p>Deep Security Firewall rules examine the control information of network packets, and determine if a network connection should be allowed. Stateful Configuration filters analyze each network packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions, managing existing network sessions with great efficiency. The Deep Security fine-grained filtering firewall rules filter traffic based on source and destination IP address, port, MAC address, etc. Different rules can be applied to different network interfaces. For end-user systems, the firewall is location aware, and is able to limit interface use such that only a single interface can be used at one time, and security profiles provide a logical way of replicating security settings to physical or virtual servers or machines that share similar security requirements.</p> <p>TippingPoint can restrict incoming communications traffic through security profiles, which define the traffic that the IPS monitors and the DV filters that the IPS applies. Traffic monitoring is based on incoming and outgoing port pairs. An organization can use the default DV filter configuration to protect the segment or customize the configuration as required. The segment specifies both the port and the traffic direction, which allows an organization to define separate security profiles for traffic in and out of a port.</p>
<p>SC-7 (12) System and Communications Protection / Boundary Protection / Host-Based Protection</p> <p>Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].</p> <p>Supplemental Guidance: Host-based boundary protection mechanisms include, for example, host-based firewalls. Examples of system components employing host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.</p>	CNSSI FedRAMP 800-171 CUI	E	<p>Deep Discovery Inspector determines host severity and the impact on a host as determined from aggregated detections by Trend Micro products and services. Investigating beyond event security, the host severity numerical scale exposes the most vulnerable hosts and allows an organization to prioritize and quickly respond. Host severity is based on the aggregation and correlation of the severity of the events that affect a host. If several events affect a host and have no detected connection, the host severity will be based on the highest event severity of those events. However, if the events have a detected correlation, the host severity level will increase accordingly.</p> <p>Deep Discovery Email Inspector assesses an organization's boundary protection for email message risk using multi-layered threat analysis. Upon receiving an email message, Deep Discovery Email Inspector email scanners check the email message for known threats in the Trend Micro Smart Protection Network and Trend Micro Advanced Threat Scanning Engine. If the email message has unknown or suspicious characteristics, the email scanners send file attachments and embedded URLs to Virtual Analyzer for further analysis. Virtual Analyzer simulates the suspicious file and URL behavior to identify potential threats. Deep Discovery Email Inspector assigns a risk level to the email message based on the highest risk assigned between the Deep Discovery Email Inspector scanners and Virtual Analyzer.</p> <p>Deep Discovery Analyzer provides boundary protection through suspicious objects, which are objects with the potential to expose systems to danger or loss. Deep Discovery Analyzer detects and analyzes suspicious IP addresses, host names, files, and URLs.</p> <p>Deep Security solution provides host-based boundary protection through the host application stateful inspection firewall, through the host deep packet inspection, and through web reputation services. This can be implemented at the server or workstation level in the physical or virtual environments. Deep Security virtual machine isolation allows VMs to be isolated virtual environments, providing virtual segmentation without the need to modify virtual switch configurations or network architecture.</p>
<p>SC-7 (16) System and Communications Protection / Boundary Protection / Prevent Discovery of Components / Devices</p> <p>Prevent the discovery of specific system components that represent a managed interface.</p> <p>Supplemental Guidance:</p>	800-171 CUI	E	<p>Deep Discovery Inspector offers sophisticated detection capabilities using multiple advanced detection engines to present detailed information about custom and signature-based threats passing through various network protocols. Deep Discovery Inspector detects targeted attacks and advanced threats, and helps remediate targeted attacks with automated processes. Deep Discovery Inspector is purpose-built for detecting APT and</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>This control enhancement protects network addresses of system components that are part of managed interfaces from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery, requiring prior knowledge for access. This can be accomplished by not publishing network addresses or entering the addresses in domain name systems. Another obfuscation technique is to periodically change network addresses.</p>		<p>targeted attacks. It identifies malicious content, communications, and behavior that may indicate advanced malware or attacker activity across every stage of the attack sequence</p> <p>Deep Discovery Email Inspector acts upon email messages according to the assigned risk level and policy settings. Deep Discovery Email Inspector can be configured to block and quarantine the email message, allow the email message to pass to the recipient, strip suspicious file attachments, redirect suspicious links to blocking or warning pages, or tag the email message with a string to notify the recipient.</p> <p>Deep Discovery Analyzer shares new IOC detection intelligence automatically with other Trend Micro solutions and third-party security products.</p> <p>Deep Security solution through the functionality of "Reconnaissance Detection" can determine and advise if an external entity is attempting to discover specific system components or weaknesses associated with them. Smart rules provide broad protection, and low-level insight, for servers and end-user systems. For operating systems and applications, the rules limit variations of elements of traffic, limiting the ability of attackers to investigate possible attack vectors since many attacks are based on exceeding expected characteristics. For servers and end-user systems, smart rules also provide insight into application activity and unexpected traffic (HTTP on an unexpected port, use of a web browser on a server, etc)</p> <p>TippingPoint - the filters within the Digital Vaccine package are developed by TippingPoint's Digital Vaccine Labs to protect the network from specific exploits as well as potential attack permutations to address for Zero-Day threats. These filters include traffic anomaly filters and vulnerability-based filters. Vulnerability-based filters are designed to protect the network from an attack that takes advantage of a weakness in application software. For viruses that are not based on a specific vulnerability in software, the DV provides signature filters. TippingPoint delivers weekly DV updates that can be automatically installed on the IPS device (System > Update). If a critical vulnerability or threat is discovered, DV updates are immediately distributed to customers.</p>
<p>SC-7 (17) System and Communications Protection / Boundary Protection / Automated Enforcement of Protocol Formats</p> <p>Enforce adherence to protocol formats.</p> <p>Supplemental Guidance:</p> <p>Examples of system components that enforce protocol formats include deep packet inspection firewalls and XML gateways. Such components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.</p> <p>Related Controls: SC-4.</p>	<p>800-171 CUI</p>	<p>Deep Discovery Inspector through the Virtual Analyzer module provides a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration. Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics such as suspicious network or messaging activity.</p> <p>Deep Discovery Email Inspector scans for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information.</p> <p>Deep Discovery Analyzer Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:</p> <ul style="list-style-type: none"> - Anti-security and self-preservation - Autostart or other system configuration - Deception and social engineering - File drop, download, sharing, or replication - Hijack, redirection, or data theft - Malformed, defective, or with known malware traits - Process, service, or memory object change - Rootkit, cloaking - Suspicious network or messaging activity <p>During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC files that can be used in investigations.</p> <p>Deep Security Intrusion prevention rules define a set of conditions that are compared to the payload session and application layers of network packets (such as DNS, HTTP, SSL, and SMTP), as well as the sequence of those packets according to those higher-layer protocols. Firewall rules examine the network and transport layers of a packet (IP, TCP, and UDP, for example). When Deep Security Agents scan network traffic and the traffic meets a rule's match conditions, the agent handles it as a possible or confirmed attack and performs one of the following actions, depending on the rule:</p> <ul style="list-style-type: none"> - Replace specifically defined or suspicious byte sequences - Completely drop packets Reset the connection <p>Deep Packet Inspection module is available in both the Deep Security Agent and Deep</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>SC-7 (17) System and Communications Protection / Boundary Protection / Automated Enforcement of Protocol Formats (... Continued.)</p>		<p>Security Appliance for VMware ESX/ESXi. Deep Packet Inspection provides an automated IDS/IPS capability, which protects operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injection and cross-site scripting.</p> <p>Firewall rules examine the control information of network packets, and determine if a network connection should be allowed. Stateful configuration filters analyze each network packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions, manages existing network sessions efficiently. The Deep Security fine-grained filtering firewall rules filter traffic based on source and destination IP address, port, MAC address, etc. Different rules can be applied to different network interfaces. For end-user systems, the firewall is location aware, and is able to limit interface use such that only a single interface can be used at one time, and security profiles provide a logical way of replicating security settings to physical or virtual servers or machines that share similar security requirements. In addition, intrusion prevention rules provide control of:</p> <ul style="list-style-type: none"> - Application Type: The application type under which this intrusion prevention rule is grouped. - Priority: The priority level of the rule. Higher priority rules are applied before lower priority rules. - Severity: Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of intrusion prevention rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. - CVSS Score: A measure of the severity of the vulnerability according the National Vulnerability Database. <p>TippingPoint - the main component of the IPS device is the Threat Suppression Engine (TSE), a custom engine that detects and blocks a broad range of attacks at wire speeds. The TSE is a flow-based network security engine, in which each packet is identified as a component of a flow and each flow is tracked in the connection table on the IPS. A flow is uniquely identified by its packet header information:</p> <ul style="list-style-type: none"> - IPv4 or IPv6 protocol (ICMP, TCP, UDP, other) - source and destination IP addresses - source and destination ports <p>The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. When a packet matches an IPS filter, the IPS handles the packets based on the action set configured on the filter. For example, if the action set is Block, then the packet is dropped and subsequent packets from the same flow are dropped without inspection. The IPS device provides default actions to block or permit traffic with options to quarantine or rate-limit traffic and to notify users or systems when an action executes. Logging options are also available to review the types of traffic being filtered by the device. An organization can customize the default action sets, or create their own based on the network requirements. The TippingPoint IPS Services configure additional ports associated with specific applications, services, and protocols to expand the range of traffic scanned by the IPS device. During the inspection process, the IPS device first scans traffic against the standard ports for listed services, and then scans traffic against the list of additional ports. An organization can configure up to 16 additional ports for each service other than HTTP. For HTTP, only eight additional ports are allowed.</p> <p>The TippingPoint Digital Vaccine includes a category of filters, Traffic Normalization, purpose built to detect violations of networking protocols defined by an RFC.</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>SC-7 (19) System and Communications Protection / Boundary Protection / Blocks Communication From Non-Organizationally Configured Hosts</p> <p>Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.</p> <p>Supplemental Guidance: Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.</p>	800-171 CUI	<p>E</p> <p>Deep Discovery Inspector viewing hosts attacked in the past 1 hour, 24 hours, 7 days, or 30 days and the type of detected attack allows users (typically system or network administrators) to take appropriate action (blocking network access, isolating computers according to IP address) to prevent malicious operations from affecting hosts.</p> <p>Deep Discovery Email Inspector simplifies preventative actions with a streamlined policy structure to block and quarantine suspicious email messages.</p> <p>Deep Discovery Analyzer determines suspicious objects, which are objects with the potential to expose systems to danger or loss. Deep Discovery Analyzer detects and analyzes suspicious IP addresses, host names, files, and URLs.</p> <p>Deep Security Firewall Rules examine the control information of network packets, and determine if a network connection should be allowed. Stateful Configuration filters analyze each network packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions, manages existing network sessions with great efficiency.</p> <p>TippingPoint - the main component of the IPS device is the Threat Suppression Engine (TSE), a custom engine that detects and blocks a broad range of attacks at wire speeds. The TSE is a flow-based network security engine, in which each packet is identified as a component of a flow and each flow is tracked in the connection table on the IPS. A flow is uniquely identified by its packet header information:</p> <ul style="list-style-type: none"> - IPv4 or IPv6 protocol (ICMP, TCP, UDP, other) - source and destination IP addresses - source and destination ports <p>The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. When a packet matches an IPS filter, the IPS handles the packets based on the action set configured on the filter. For example, if the action set is Block, then the packet is dropped and subsequent packets from the same flow are dropped without inspection. The IPS device provides default actions to block or permit traffic with options to quarantine or rate-limit traffic and to notify users or systems when an action executes. Logging options are also available to review the types of traffic being filtered by the device. An organization can customize the default action sets, or create their own based on the network requirements.</p>
<p>SC-7 (20) System and Communications Protection / Boundary Protection / Dynamic Isolation / Segregation</p> <p>Provide the capability to dynamically isolate or segregate [Assignment: organization-defined system components] from other system components.</p> <p>Supplemental Guidance: The capability to dynamically isolate or segregate certain internal components of organizational systems is useful when it is necessary to partition or separate certain system components of questionable origin from those components possessing greater trustworthiness. Component isolation reduces the attack surface of organizational systems. Isolating selected system components can also limit the damage from successful attacks when such attacks occur.</p>	FedRAMP 800-171 CUI	<p>E</p> <p>Deep Discovery Inspector detects and identifies evasive threats in real-time, and provides in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.</p> <p>Deep Discovery Email Inspector provides real-time threat visibility and analysis in a multi-level format. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures. Deep Discovery Email Inspector makes use of the Virtual Analyzer module, an isolated virtual environment used to manage and analyze samples. Virtual Analyzer observes sample behavior and characteristics, and then assigns a risk level to the sample.</p> <p>Deep Discovery Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. Deep Discovery Analyzer can be used to augment or centralize the sandbox analysis of other products. The custom sandboxing environments that can be created within Deep Discovery Analyzer precisely match target desktop software configurations — resulting in more accurate detections and fewer false positives.</p> <p>Deep Security firewall can be used to create the implied Trust Zone architectures in physical and virtualized environments. Deep Security also supports this requirement in virtual environment by its support of VMware's NSX tagging of infected virtual machines that allows for the virtual machines to be automatically quarantined.</p> <p>TippingPoint - the LSM enables an organization to view and modify the setup of the IPS device so that it can work within the enterprise network environment. The following options are available:</p> <ul style="list-style-type: none"> - <u>Segments</u> — View and manage segment configuration for Layer-2 Fallback (high availability) and link down synchronization. - <u>Network Ports</u> — Disable, enable, or restart a port, and manage port configuration (auto-negotiation and line speed). - <u>Virtual Ports</u> — Create and manage virtual ports that logically classify the network by transport ports, CIDR (Classless Inter-Domain Routing) addresses, and VLAN IDs so that IPS filtering can be applied to the traffic. - <u>Virtual Segments</u> — Create and manage virtual segments to further refine the

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
			<p>network traffic classifications.</p> <ul style="list-style-type: none"> - <u>VLAN Translation</u> — Enable translation of traffic between different VLANs or between VLAN and non-VLAN interfaces. - <u>Network Tools</u> — Review the types of traffic that the network is receiving.
<p>SC-7 (21) System and Communications Protection / Boundary Protection / Isolation of Information System Components</p> <p>Employ boundary protection mechanisms to separate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].</p> <p>Supplemental Guidance: Organizations can isolate system components performing different missions or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from hostile attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks; cross-domain devices separating subnetworks; virtualization techniques; and encrypting information flows among system components using distinct encryption keys.</p> <p>Related Controls: CA-9, SC-3.</p>			
	H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Security firewall can be used to create the implied Trust Zone architectures in a physical and virtualized environments. Deep Security also supports this requirement in virtual environment by its support of VMware's NSX tagging of infected virtual machines that allows for the virtual machines to be automatically quarantined. Information flow control in a multi-tenant cloud environment, to ensure the protection and boundary control of an organizations data, in an environment where boundary protection is generally considered to be very important.</p> <p>TippingPoint - the LSM enables an organization to view and modify the setup of the IPS device so that it can work within the enterprise network environment. The following options are available:</p> <ul style="list-style-type: none"> - <u>Segments</u> — View and manage segment configuration for Layer-2 Fallback (high availability) and link down synchronization. - <u>Network Ports</u> — Disable, enable, or restart a port, and manage port configuration (auto-negotiation and line speed). - <u>Virtual Ports</u> — Create and manage virtual ports that logically classify the network by transport ports, CIDR (Classless Inter-Domain Routing) addresses, and VLAN IDs so that IPS filtering can be applied to the traffic. - <u>Virtual Segments</u> — Create and manage virtual segments to further refine the network traffic classifications. - <u>VLAN Translation</u> — Enable translation of traffic between different VLANs or between VLAN and non-VLAN interfaces. - <u>Network Tools</u> — Review the types of traffic that the network is receiving <p>TippingPoint Threat Management Center provides Infrastructure Protection — which protects network bandwidth and network infrastructure elements, such as routers and firewalls, from attack using a combination of filter types:</p> <ul style="list-style-type: none"> - <u>Advanced DDoS filters</u> — Available on the 2400E and 5000E. Detect and block denial of service and flood requests, such as SYN Requests, that can overwhelm a system. - <u>Network Equipment Protection filters</u> — Protect networked equipment from attacks. - <u>Traffic Normalization filters</u> — Detect and block abnormal or malicious traffic.

SC-8 System and Communications Protection / Transmission Confidentiality and Integrity

SC-8 System and Communications Protection / Transmission Confidentiality and Integrity

Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.

Supplemental Guidance:
This control applies to internal and external networks and any system components that can transmit information including, for example, servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical means or by logical means. Physical protection can be achieved by employing protected distribution systems. Logical protection can be achieved by employing encryption techniques. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services, may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating security controls or explicitly accept the additional risk.

Related Controls: AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SC-7, SC-16, SC-20, SC-23, SC-28. References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113, 800-177; NIST Interagency Report 8023.

M H
CNSSI
FedRAMP
800-82 ICS
800-171 CUI

P

Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, Deep Security, and TippingPoint use TLS/SSL to provide confidentiality and integrity protection when communications between the various components and services of the products is required. When a remote console connection is required the SSH protocol is used.

CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) “provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.” Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.

The Deep Security CC Security Targets includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the **SC-8** control:

- **FPT_ITT.1** (Protection of the TSF/ Internal TOE TSF Data Transfer/ Basic Internal TSF Data Transfer Protection)

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>SC-8 (1) System and Communications Protection / Transmission Confidentiality and Integrity / Cryptographic or Alternate Physical Protection</p> <p>Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.</p> <p>Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.</p> <p>Related Controls: SC-13.</p>	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>TippingPoint uses SSLimSecure 3.0 from TeamF1 for its SSL support. This library is based on OpenSSL 0.9.8b, was ported by TeamF1 to run under vxWorks, and has been subsequently patched. TippingPoint uses SSHield 2.2.0 from TeamF1 for its SSH support. This library is based on OpenSSH 3.5p1, was ported by TeamF1 to run under vxWorks, and has also been subsequently patched.</p> <p>TippingPoint supports two modes of FIPS operation—crypto and full. When configured in either FIPS mode, TippingPoint will allow only FIPS 140-2 (Certificate # 2391) approved cryptographic algorithms to be used.</p> <p>----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>“provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.”</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security CC Security Target includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the SC-8 (1) control:</p> <ul style="list-style-type: none"> - FPT_ITT.1 (<i>Protection of the TSF/ Internal TOE TSF Data Transfer/ Basic Internal TSF Data Transfer Protection</i>)

SC-11 System and Communications Protection / Trusted Path

SC-11 System and Communications Protection / Trusted Path <p>a. Provide a [Selection: physically; logically] isolated trusted communications path for communications between the user and the trusted components of the system; and</p> <p>b. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [Assignment: organization-defined security functions].</p> <p>Supplemental Guidance: Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of systems with the requisite assurance to support security policies. These mechanisms can be activated only by users or the security functions of organizational systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for trustworthy, high-assurance connections between security functions of systems and users including, for example, during system logons. The original implementations of trusted path used an out-of-band signal to initiate the path, for example using the <BREAK> key, which does not transmit characters that can be spoofed. In later implementations, a key combination that could not be hijacked was used, for example, the <CTRL> + <ALT> + keys. Note, however, that any such key combinations are platform-specific and may not provide a trusted path implementation in every case. Enforcement of trusted communications paths is typically provided by a specific implementation that meets the reference monitor concept.</p> <p>Related Controls: AC-16, AC-25, SC-12, SC-23.</p>		P	<p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>“provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53.”</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The TippingPoint CC Security Target includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the SC-11 control:</p> <ul style="list-style-type: none"> - FPT_TRP.1 (<i>Trusted Path Channels/ Trusted Path</i>)
---	--	---	--

SC-12 System and Communications Protection / Cryptographic Key Establishment and Management

SC-12 System and Communications Protection / Cryptographic Key Establishment and Management <p>Establish and manage cryptographic keys for required cryptography employed within the system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].</p> <p>Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define their key management requirements in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems.</p> <p>Related Controls: AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-9, SC-8, SC-11, SC-</p>	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Security has obtained FIPS 140-2 certification for the Trend Micro Cryptographic Module and the Trend Micro Java Crypto Module, see:</p> <ul style="list-style-type: none"> - Trend Micro Java Crypto Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3140 - Trend Micro Cryptographic Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3125 <p>TippingPoint Security Management System (SMS) implements a FIPS 140-2 certified module (Certificate # 2391) to manage cryptographic keys.</p>
---	--	---	--

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7. References: NIST Special Publications 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 95663; NIST Interagency Reports 7956, 7966.</p> <p>SC-12 (2) System and Communications Protection / Cryptographic Key Establishment and Management / Symmetric Keys Produce, control, and distribute symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes.</p> <p>SC-12 (3) System and Communications Protection / Cryptographic Key Establishment and Management / Asymmetric Keys Produce, control, and distribute asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved DoD PKI Class 3 certificates; prepositioned keying material; approved DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements].</p>	FedRAMP 800-171 CUI		
<p>SC-13 System and Communications Protection / Cryptographic Protection</p> <p>SC-13 System and Communications Protection / Cryptographic Protection Implement the following cryptographic uses and type of cryptography for each use: [Assignment: organization-defined cryptographic uses and type of cryptography required for each use].</p> <p>Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified information and Controlled Unclassified Information; the provision and implementation of digital signatures; and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required due to the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required. For example, organizations that need to protect classified information specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures specify the use of FIPS-validated cryptography. In all instances, cryptography is implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.</p> <p>Related Controls: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7. References: FIPS Publication 140-2.</p>	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	P	<p>Deep Security Deep Security has obtained FIPS 140-2 certification for the Trend Micro Cryptographic Module and the Trend Micro Java Crypto Module, see:</p> <ul style="list-style-type: none"> - Trend Micro Java Crypto Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3140 - Trend Micro Cryptographic Module: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3125 <p>TippingPoint Security Management System (SMS) implements a FIPS 140-2 certified module to provide cryptographic protection.</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) "provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53." Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security CC Security Target includes the following control which is mapped (in SP 800-53 Table I-3) to supporting the SC-13 control:</p> <ul style="list-style-type: none"> - FCS_COP.1 (Cryptographic Support/ Cryptographic Operation)
<p>SC-18 System and Communications Protection / Mobile Code</p> <p>SC-18 (3) System and Communications Protection / Mobile Code / Prevent Downloading / Execution Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].</p>	CNSSI 800-171 CUI	E	<p>Deep Discovery Inspector detects targeted attacks and advanced threats and helps remediate targeted attacks with automated processes. Deep Discovery Inspector accesses the Mobile App Reputation Service (MARS) to obtain information about emerging mobile threats. MARS collects data about detected threats in mobile devices. Mobile App Reputation Service is an advanced sandbox environment that analyzes mobile app runtime behavior to detect privacy leaks, repacked mobile apps, third-party advertisement SDKs, vulnerabilities, and app categories. The Deep Discovery Inspector Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in mobile code software such as Java and Flash.</p> <p>Deep Discovery Email Inspector can be configured to use the internal or external Virtual Analyzer sandbox environment. When simulating file and URL behavior, Virtual Analyzer uses its own analysis engine to determine the risk of an object. Virtual Analyzer can scan for a variety of file types, including Flash and other multimedia, Java, Scripts including javascript files.</p> <p>Deep Discovery Email Inspector quarantines suspicious email messages that meet certain policy criteria. Use is also made of the Script Analyzer Engine. The Script Analyzer Engine analyzes web page scripts to identify malicious code and the Script Analyzer</p>

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
SC-18 (3) System and Communications Protection / Mobile Code / Prevent Downloading / Execution (... Continued.)			<p>Pattern is used during analysis of webpage scripts to identify malicious mobile code. Deep Discovery Analyzer can detect mobile code such as java, javascripts, and flash multimedia these can be tagged as suspicious objects and an alert notification issued.</p> <p>Deep Security can check whether a file contains script (JavaScript, PHP, or ASP script) and block.</p> <p>TippingPoint can protect a system against mobile code (java, javascript, flash multimedia) attack through the implementation of the DV filters which are contained in a Digital Vaccine (DV) package. All IPS devices have a DV package installed and configured to provide out-of-the-box IPS protection for the network. The filters within the DV package are developed by TippingPoint's Digital Vaccine Labs to protect the network from specific exploits as well as potential attack permutations to address for Zero-Day threats. These filters include traffic anomaly filters and vulnerability-based filters. Vulnerability-based filters are designed to protect the network from an attack that takes advantage of a weakness in application software. For viruses that are not based on a specific vulnerability in software, the DV provides signature filters. Tipping Point delivers weekly DV updates that can be automatically installed on the IPS device</p>

SC-28 System and Communications Protection / Protection of Information at Rest

SC-28 System and Communications Protection / Protection of Information At Rest
Protect the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information] at rest.
Supplemental Guidance:
This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of this control is not on the type of storage device or frequency of access but rather the state of the information. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection and prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other security controls including, for example, frequent scanning to identify malicious code at rest and secure off-line storage in lieu of online storage.
Related Controls: AC-3, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-13, SC-34, SI-3, SI-7, SI-16.
References: NIST Special Publications 800-56A, 800-56B, 800-56C, 800-57-1, 800-57-2, 800-57-3, 800-111, 800-124.

M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Security solution provides Integrity Monitoring of critical systems related information detecting when a systems critical configuration file or rule set has been modified. The Deep Security Application Control module monitors changes — “drift” or “delta” — compared to the computer’s original software. Once application control is enabled, all software changes are logged and events are created when it detects new or changed software on the file system. When Deep Security Agent detects changes, an organization can allow or block the software, and optionally lock down the computer.</p>
--	---	---

SC-32 System and Communications Protection / Information System Partitioning

SC-32 System and Communications Protection / Information System Partitioning
Partition the system into [Assignment: organization-defined system components] residing in separate physical domains or environments based on [Assignment: organization-defined circumstances for physical separation of components].
Supplemental Guidance:
System partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.
Related Controls: AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36.
References: FIPS Publication 199.

800-171 CUI	E	<p>Deep Security solution provides, through the firewall functionality, an ability to create Trust Zones in a physical or virtualized environment. The Deep Packet Inspection provides flow control between the various machines either physical or virtualized in the different Trust Zones.</p> <p>TippingPoint Threat Suppression Engine (TSE) is a line-speed hardware engine that contains all the functions needed for Intrusion Prevention, including flow blocking and flow state tracking. The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The blocking of the traffic and packets ensures that the attack never reaches its destination.</p>
-------------	---	---

SC-36 System and Communications Protection / Distributed Processing and Storage

SC-36 System and Communications Protection / Distributed Processing and Storage Distribute [Assignment: organization-defined processing and storage components] across multiple physical locations. Supplemental Guidance: Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and therefore, allows for parallel processing and storage. Related Controls: CP-6, CP-7, PL-8, SC-32.	800-171 CUI	E	When an organization distributes the processing and storage across multiple physical locations a significant issue is to have the processing and storage security synchronized with the machines in the different locations. To this end, Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Analyzer, Deep Security, and TippingPoint through the promulgation of security policies, profiles, and firewall rules from central management services provided by Control Manager and the Security Management System can ensure that machines located in different locations have the correct security policies and safeguards implemented for their Trust Zone level.
---	-------------	---	--

SC-44 System and Communications Protection / Detonation Chambers

SC-44 System and Communications Protection / Detonation Chambers Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location]. Supplemental Guidance: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, this control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely. Related Controls: SC-7, SC-25, SC-26, SC-30, SC-35, SI-3, SI-7. References: NIST Special Publication 800-177.	800-171 CUI	E	Deep Discovery Inspector, and Deep Discovery Email Inspector through the Virtual Analyzer module meets this requirement by providing advanced and customizable sandboxing for the "detonation" of suspicious files and applications detected between or within networks across all ports and the 80+ most common protocols in use by organizations. Deep Discovery Analyzer meets this requirement by providing advanced and customizable sandboxing for the "detonation" of suspicious files and applications detected between or within networks across all ports and the 80+ most common protocols in use by organizations. Deep Security through the Connected Threat Defense capability, the Deep Security Agent uses heuristic detection to analyze files on the protected computer and determines whether they are suspicious. Suspicious files from Deep Security can manually or automatically be sent to Deep Discovery Analyzer, which executes and observes the suspicious file in a sandbox (a secure, isolated virtual environment). Deep Security Manager gets the sandbox analysis results from Deep Discovery Analyzer.
--	-------------	---	---

SI-2 System and Information Integrity / Flaw Remediation

SI-2 System and Information Integrity / Flaw Remediation a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time-period] of the release of the updates; and d. Incorporate flaw remediation into the organizational configuration management process. Supplemental Guidance: Organizations identify systems affected by software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into ongoing configuration management processes, required remediation actions can be tracked and verified. Organization-defined time-periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that testing of software or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P	Deep Discovery Inspector supports this control through providing firmware updates, which address flaws, and are configurable in the administration console. Deep Discovery Inspector product components used to scan for and detect network threats can be frequently updated as Trend Micro creates new component versions, perform regular updates to address the latest threats and flaws. There are a number of Trend Micro components that assist with this control, such as the : - Advanced Persistent Threat Information Pattern which provides details about advanced persistent threats. - Advanced Threat Correlation Pattern which contains a list of file features that are not relevant to any known threats. - Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature-based behavior-based, and aggressive heuristic detection. - Common Vulnerabilities and Exposures Information Pattern provides CVE reference information for detections. Deep Discovery Email Inspector Trend Micro frequently creates new component versions, perform regular updates to address the latest spear-phishing attacks and social engineering attack patterns. Deep Discovery Analyzer updates on a regular basis key components to assist with flaw remediation, these key components are: - The Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature based, behavior-based, and aggressive heuristic detection. - The Deep Discovery Malware Pattern contains information that helps Deep Discovery Analyzer identify the latest malware and mixed threat attacks. Trend Micro creates and releases new versions of the pattern several times a week, and any time after the discovery of a particularly damaging virus/malware.
--	--	-----	--

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>Related Controls: CA-4, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.</p> <p>References: FIPS Publications 140-2, 186-4; NIST Special Publications 800-40, 800-128; NIST Interagency Report 7788.</p>			<ul style="list-style-type: none"> - Network Content Inspection Pattern is used by the Network Content Inspection Engine to perform network scanning. - The Spyware/Grayware Pattern identifies unique patterns of bits and bytes that signal the presence of certain types of potentially undesirable files and programs, such as adware and spyware, or other grayware. <p>Deep Security, Recommendation Scan supports this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits.</p> <p>Deep Security also has Anti-malware capabilities that use the latest techniques to identify and remediate malware incidents on a particular host. This includes advanced detections such as predictive machine learning and behavioral analysis. This control can quarantine, clean or delete malware files depending on the configured settings.</p> <p>TippingPoint through the Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation. The TMC collects threat information and creates Digital Vaccine packages that are made available on the TMC website. The packages include filters that block malicious traffic and attacks on the organizations network.</p> <p>----</p> <p>CC Security Targets identify functional and assurance requirements to be addressed in the CC evaluations. SP 800-53 (Table I-3) <i>"provides a generalized mapping from the functional and assurance requirements in ISO/IEC 15408 (Common Criteria) to the controls in NIST Special Publication 800-53."</i> Such mappings indicates which evaluated CC controls will assist in supporting specific SP 800-53 controls.</p> <p>The Deep Security, Deep Discovery Inspector, and TippingPoint CC Security Targets include the following controls which are mapped (in SP 800-53 Table I-3) to supporting the SI-2 control:</p> <ul style="list-style-type: none"> - ALC_FLR.1 (<i>Life-Cycle Support/ Flaw Remediation/ Basic Flaw Remediation</i>) – Deep Security; - ALC_FLR.2 (<i>Life-Cycle Support/ Flaw Remediation/ Flaw Reporting Procedure</i>) – Deep Discovery Inspector & TippingPoint.

SI-3 System and Information Integrity / Malicious Code Protection

<p>SI-3 System and Information Integrity / Malicious Code Protection</p> <ol style="list-style-type: none"> a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: <ol style="list-style-type: none"> 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system. <p>Supplemental Guidance:</p> <p>System entry and exit points include, for example, firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including, for example, by electronic mail, the world-wide web, and portable storage devices. Malicious code</p>	<p>L M H</p> <p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>E</p>	<p>Deep Discovery Inspector supports this control for malicious code protection. Deep Discovery Inspector detection engines deliver expanded APT and targeted attack detection including custom virtual analyzer and new discovery and correlation rules designed to detect malicious content, communication, and behavior across every stage of an attack sequence. The Advanced Threat Scan Engine is an upgrade from the standard virus scan engine, which protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature-based, behavior-based, and aggressive heuristic detection. Major features include the following: <ul style="list-style-type: none"> - Detection of zero-day threats; - Detection of embedded exploit code; - Detection rules for known vulnerabilities; - Enhanced parsers for handling file deformities. The Deep Discovery Inspector Virtual Analyzer is a secure virtual environment used to manage and analyze suspicious network and file samples. Sandbox images allow observation of file and network behavior in a natural setting without any risk of compromising the network. Virtual Analyzer performs static analysis and behavior simulation to identify potentially malicious characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings.</p> <p>Deep Discovery Inspector connects to Trend Micro products and hosted services to update components by connecting to the ActiveUpdate server. Trend Micro regularly creates new component versions, and performs regular updates (signatures, patterns) to address the latest threats. Deep Discovery Inspector downloads components from the Trend Micro ActiveUpdate server, the default update source for the latest components. These components are:</p>
---	--	----------	---

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Malicious code protection mechanisms include, for example, signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include, for example, artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against such code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software and in custom-built software. This could include, for example, logic bombs, back doors, and other types of attacks that could affect organizational missions and business functions.</p> <p>In situations where malicious code cannot be detected by detection methods and technologies, organizations rely instead on other types of safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, or actions in response to detection of maliciousness when attempting to open or execute files. Due to system integrity and availability concerns, organizations consider the specific methodology used to carry out automatic updates.</p> <p>Related Controls: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, RA-5, SC-7, SC-26, SC-28, SC-23, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.</p>		<ul style="list-style-type: none"> - Advanced Threat Scan Engine, - Advanced Persistent Threat Information Pattern - Advanced Threat Correlation Pattern - C&C Identification Pattern - Common Threat Family Information Pattern - Common Vulnerability and Exposure Information Pattern - Contextual Intelligence Query Handler - Deep Discovery Malware Pattern - IntelliTrap Pattern, - IntelliTrap Exception Pattern, - Network Content Correlation Pattern, - Network Content Inspection Engine, - Network Content Inspection Pattern, - Script Analyzer Pattern - Spyware/Grayware Pattern - Threat Correlation Pattern, - Threat Knowledge Base, - Trend Micro Intelligence Agent v.2 - Trusted Certificate Authorities Pattern - Virtual Analyzer Configuration Pattern - Virtual Analyzer Sensors. <p>Deep Discovery Email Inspector investigates email messages for suspicious file attachments, embedded links (URLs), and characteristics. If an email message exhibits malicious behavior, Deep Discovery Email Inspector can block the threat and notify security administrators about the malicious activity. After investigating email messages, Deep Discovery Email Inspector assesses the risk using multi-layered threat analysis. Deep Discovery Email Inspector calculates the risk level based on the highest risk assigned between the Deep Discovery Email Inspector email scanners and Virtual Analyzer. The Deep Discovery Email Inspector Virtual Analyzer sandbox environment opens files, including password-protected archives and document files, and URLs to test for malicious behavior. Virtual Analyzer is able to find exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.</p> <p>Deep Discovery Email Inspector through the Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature based, behavior-based, and aggressive heuristic detection. In addition, the Deep Discovery Malware Pattern contains the detection routines for virus and malware scanning. Trend Micro updates the Deep Discovery Malware Pattern regularly with detection routines for new identified threats. Frequently update components to receive protection from the latest threats. By default, components automatically receive updates from the Trend Micro ActiveUpdate server. The components which are updated include:</p> <ul style="list-style-type: none"> - Advanced Threat Scan Engine, - Deep Discovery Malware Pattern, - Deep Discovery Trusted Certificate Authorities Pattern, - IntelliTrap Pattern, - IntelliTrap Exception Pattern, - Network Content Correlation Pattern, - Network Content Inspection Engine, - Network Content Inspection Pattern, - Script Analyzer Engine, - Script Analyzer Pattern, - Spyware/Grayware Pattern, - Virtual Analyzer Sensors. - Virtual Analyzer Configuration Pattern.
<p>SI-3 System and Information Integrity / Malicious Code Protection</p> <p>(Continued: Deep Security)</p>		<p>Deep Security Anti-Malware module protects Windows and Linux workloads against malicious software, such as malware, spyware, and Trojans. Powered by the Trend Micro Smart Protection Network, the Anti-Malware module helps to instantly identify and remove malware and blacklist domains known to be command and control servers. The Anti-Malware can be configured to provide:</p> <ul style="list-style-type: none"> - The applicable real-time policies that apply during different periods of the day/week; - The policy for full scheduled or manual scans; - Exclusions of file types and directories; and - Real-time behavior (scanning reads and/or writes) and applicable actions. <p>Upon detection of a file-based virus, Deep Security performs the actions specified by</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
		<p>the authorized administrator. Actions are administratively configurable on a virtual or physical machine and consist of:</p> <ul style="list-style-type: none"> - Clean the virus from the file, - Quarantine the file, and - Delete the file. <p>The Deep Security, Intrusion Prevention Module is both a host based Intrusion Detections System (IDS) and an Intrusion Prevention System (IPS) which protects host computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network. Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets.</p> <p>Deep Security is able to collect an audit event from a computer indicating detection of a virus. The event identifies the computer originating the audit event, the virus that was detected and the action taken by the Deep Security. Deep Security sends an alarm to the authorized administrator and records the attempt as a system data record.</p> <p>Deep Security can apply NSX Security Tags to protected VMs upon detecting a malware threat. Further support for compliance with this requirement is achieved through the Trend Micro Smart Protection Network, which uses a global network of threat intelligence sensors to continually update email, web, and file reputation databases in the cloud, identifying and blocking threats in real time before they reach the organization requiring the protection.</p> <p>Deep Security performs real-time, scheduled, and on-demand scans for file-based viruses based upon known signatures and to automatically update and apply Deep Security signatures, engines, patterns, and rules/filters to detect/prevent exploitation of these vulnerabilities and to produce reports which can be used to support continuous monitoring. The Deep Security solution implements within the anti virus and deep packet inspection functionality heuristic techniques to compliment the signature based techniques more commonly used.</p>
<p>SI-3 System and Information Integrity / Malicious Code Protection</p> <p>(Continued: TippingPoint)</p>		<p>Tipping Point Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation. The TMC collects threat information and creates Digital Vaccine packages that are made available on the TMC website. The packages include filters that block malicious traffic and attacks on an organizations network. The filters provide the following protections:</p> <ul style="list-style-type: none"> - Application Protection — Defend against known and unknown exploits that target applications and operating systems; - Attack Protection filters — Detect and block traffic known to be malicious, suspicious, and to have known security implications. These filters include vulnerabilities and exploits filters. - Security Policy filters — Detect and block traffic that might or might not be malicious. This traffic might be different in its format or content from standard business practice, aimed at specific software or operating systems, or contrary to an organization's security policies. - Reconnaissance filters — Detect and block scans, sweeps, and probes for vulnerabilities and information about the organization's network. These filters include probes and sweeps/scans filters. - Informational filters — Detect and block classic Intrusion Detection System (IDS) infiltration
<p>SI-3 System and Information Integrity / Malicious Code Protection</p> <p>(Continued: other key products and services)</p>		<p>Compliance to the complex and challenging SI-3 <i>Malicious Code Protection</i> requirements are also supported by other key Trend Micro services and products including the following. (High level functional descriptions are provided in Section 1. Introduction.) :</p> <ul style="list-style-type: none"> - Deep Discovery Analyzer (section 1.1.1); - Deep Discovery Director (section 1.1.1); - TrendLabs (section (section 1.1.4); - Web Reputation Services (section 1.1.4).

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy	
SI-3 (1) System and Information Integrity / Malicious Code Protection / Central Management Centrally manage malicious code protection mechanisms. Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw and malicious code protection controls. Related Controls: PL-9.		M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	<p>Deep Discovery Inspector supports this control by providing central management through the Management Console and the Control Manager to provide a software management solution that gives an organization the ability to control antivirus and content security programs from a central location, regardless of the Deep Discovery Inspector's physical location or platform. Deep Discovery Inspector can simplify the administration of a corporate antivirus and content security policy through central management. Deep Discovery Inspector connects to Trend Micro products and hosted services to update components by connecting to the Active Update server. Trend Micro regularly creates new component versions, and performs regular updates (signatures, patterns) to address the latest threats.</p> <p>Deep Discovery Email Inspector makes use of Deep Discovery Director support which provides centralized Virtual Analyzer image deployment and configuration replication. Also the Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for managed products and services throughout the network.</p> <p>Deep Discovery Analyzer provides sandboxing as a centralized service which ensures optimized performance with a scalable solution able to keep pace with email, network, endpoint, and any additional source of samples.</p> <p>Deep Security solution centrally manages the malicious code protection mechanisms either the anti-virus or the deep packet inspection through the Deep Security Manager. Deep Security employs automatic update mechanisms to signatures, patterns, and rules. The Deep Security Manager, through the centralized web-based management console, permits administrators to configure security policy and deploy protection to the enforcement points. Deep Packet Inspection rules and filters, can also be integrated in the VMware environment with the vCenter Server providing a systems administrator with a single view point of anti-virus and malicious code activity.</p> <p>Tipping Point makes use of the SMS Server as an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for well over a hundred Tipping Point IPS devices. The Tipping Point Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation. The TMC collects threat information and creates Digital Vaccine packages that are made available on the TMC website. The packages include filters that block malicious traffic and attacks on an organization's network.</p>	
SI-3 (4) System and Information Integrity / Malicious Code Protection / Updates Only by Privileged Users Update malicious code protection mechanisms only when directed by a privileged user. Supplemental Guidance: This control enhancement is employed in situations where for reasons of security or operational continuity, updates to malicious code protection mechanisms are only applied when approved by designated organizational personnel. Related Controls: CM-5.		800-171 CUI	E P	<p>Deep Discovery Inspector supports this control through native role-based admin. Administrative accounts are allowed to update malicious code protection components. Furthermore, centralized management systems such as Trend Micro Control Manager allows for finer grain control over user access to individual product configurations.</p> <p>Deep Discovery Email Inspector uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to the accounts and present them with only the tools and permissions necessary to perform specific tasks. Each account is assigned a specific role. A role defines the level of access to the management console. Users log on to the management console using custom user accounts.</p> <p>Deep Discovery Analyzer controls updates through role-based administration and associated permissions:</p> <ul style="list-style-type: none"> - Administrator: Users have full access to submitted objects, analysis results, and product settings - Investigator: Users have read-only access to submitted objects, analysis results, and product settings, but can submit objects and download the investigation package, including submitted objects - Operator: Users have read-only access to submitted objects, analysis results, and product settings. <p>Deep Security the Deep Security Manager controls all updates to the Deep Security system, which control anti-virus or malicious code intrusion detection and prevention mechanism. Only users with escalated privileges can access the Deep Security Manager.</p>	

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy
SI-3 (4) System and Information Integrity / Malicious Code Protection / Updates Only by Privileged Users (... Continued.)				<p>Tipping Point uses role based access control to control updates there are three access levels for each user account:</p> <ul style="list-style-type: none"> - Operator — Base-level administrator user who monitors the system and network traffic. - Administrator — Enhanced administrator user who can view, manage, and configure functions and options in the system. - Super user — Administrator user who has full access to all LSM and CLI functions. <p>Common Criteria Security Targets include "extended functions" which are security requirements not found in the Common Criteria. The "extensions" in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-3 (4):</p> <ul style="list-style-type: none"> Deep Discovery Inspector: <ul style="list-style-type: none"> IDS_RDR.1,EXT - IDS Requirements / Restricted Data Review Deep Security: <ul style="list-style-type: none"> IDS_RDR.1,EXT - IDS Requirements / Restricted Data Review TippingPoint: <ul style="list-style-type: none"> IDS_RDR_EXT.1 - IDS / Data Review IDS_SDC_EXT.1 - IDS / Data Collection
SI-3 (8) System and Information Integrity / Malicious Code Protection / Detect Unauthorized Commands Detect [Assignment: organization-defined unauthorized operating system commands] through the kernel application programming interface at [Assignment: organization-defined system hardware components] and [Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command]. Supplemental Guidance: This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. Unauthorized operating system commands include, for example, commands for kernel functions from system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can define hardware components by component type, component, component location in the network, or combination therein. Organizations may select different actions for different types, classes, or instances of malicious commands. Related Controls: AU-2, AU-6, AU-12.	800-171 CUI	E		<p>Deep Discovery Inspector can detect unauthorized operating system commands targeting the kernel application programming interface. This has been demonstrated with detection of the Bashdoor/Shellshock vulnerability bug in the Bash shell. Deep Discovery Inspector can detect unauthorized commands through the following detection capabilities:</p> <ul style="list-style-type: none"> - Malicious Content - Malicious Behavior - Suspicious Behavior - Exploit - Grayware - Malicious URL - Disruptive Application - Correlated Incident <p>Deep Discovery Email Inspector can detect unauthorized commands through the detection of malicious software used by attackers to disrupt, control, steal, cause data loss, spy upon, or gain unauthorized access to computer systems</p> <p>Deep Discovery Analyzer can detect unauthorized commands by performing static and dynamic analysis to identify an object's notable characteristics in the following categories:</p> <ul style="list-style-type: none"> - Anti-security and self-preservation - Autostart or other system configuration - Deception and social engineering - File drop, download, sharing, or replication - Hijack, redirection, or data theft - Malformed, defective, or with known malware traits - Process, service, or memory object change - Rootkit, cloaking - Suspicious network or messaging activity <p>Deep Security can prevent the execution of malicious commands, file or actions. The Deep Security solution implements deep packet inspection functionality to determine when suspect commands are being received by the targeted physical or virtual machine. In the event that a suspicious activity or series of commands are issued an alert is sent to the Deep Security Manager or the SIEM system to inform the systems administrator of the security event taking place. Further, the implementation of the Deep Security Integrity Monitoring supports satisfying this requirement through ensuring that configuration files and specific commands have not been modified prior to execution.</p> <p>Deep Security also has Anti-malware capabilities that use the latest techniques to identify and prevent malicious code from being executed on a particular host. This includes advanced detections such as predictive machine learning and behavioral</p>

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy
SI-3 (8) System and Information Integrity / Malicious Code Protection / Detect Unauthorized Commands (... Continued.)				<p>analysis. This control can quarantine, clean or delete malware files depending on the configured settings.</p> <p>The Deep Security Application Control module monitors software changes — “drift” or “delta” — compared to the computer’s original software. Once application control is enabled, all software changes are logged and events are created when it detects new or changed software on the file system. When Deep Security Agent detects changes, an organization can allow or block the software, and optionally lock down the computer.</p> <p>Tipping Point through the Threat Suppression Engine (TSE) can prevent the execution of malicious commands. The TSE uses Digital Vaccine (DV) filters to police the network and to screen out malicious or unwanted traffic. In addition to the DV filters, the IPS also provides Traffic Management filters, which are custom filters that react to traffic based on source IP address, destination IP address, port, protocol, or other defined values. Traffic management filters are applied to traffic before DV filters. Depending on how the filters are configured, traffic might or might not require further inspection.</p> <p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-3 (8):</p> <ul style="list-style-type: none"> Deep Discovery Inspector: <ul style="list-style-type: none"> IDS_RDR.1,EXT - IDS Requirements / Restricted Data Review IDS_STG.1,EXT - IDS Requirements / Guarantee of System Data Availability Deep Security: <ul style="list-style-type: none"> IDS_RDR.1,EXT IDS Requirements / Restricted Data Review IDS_STG.1,EXT IDS Requirements / Guarantee of System Data Availability TippingPoint: <ul style="list-style-type: none"> DS_RDR_EXT.1 Intrusion Detection System (IDS) / IDS Data Review IDS_STG_EXT.1 Intrusion Detection System (IDS) / ISD Data Storage
SI-3 (10) System and Information Integrity / Malicious Code Protection / Malicious Code Analysis (a) Employ [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of malicious code; and (b) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes. Supplemental Guidance: The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates more effective organizational responses to current and future threats. Organizations can also conduct malicious code analyses by using reverse engineering techniques or by monitoring the behavior of executing code.	CNSSI 800-171 CUI	E P		<p>Deep Discovery Inspector provides an understanding of the characteristics of malicious code, which facilitates more effective organizational responses to current and future threats, by identifying malicious files and applications using advanced nonsignature-based detection mechanisms such as heuristics engines as well as customizable sandboxing techniques to detect, analyze and describe the characteristics or behavior of malicious code including advanced targeted and zero day malware. Deep Discovery Inspector can provide this information to other Trend products or third party security appliances such as firewalls and intrusion protection devices. The Deep Discovery Inspector Virtual Analyzer module is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match the system configuration. Virtual Analyzer performs static and dynamic analysis to identify an object’s notable security characteristic.</p> <p>Deep Discovery Email Inspector makes use of the Virtual Analyzer to analyze malicious code. The Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, and administrators and investigators (through SSH). Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration. Virtual Analyzer performs static and dynamic analysis to identify an object’s notable characteristics. When an email message enters a network, Deep Discovery Email Inspector gathers security intelligence from several Trend Micro Smart Protection Network services to investigate the email message’s risk level.</p> <ul style="list-style-type: none"> - Analyzing file attachments - Analyzing embedded links (URLs) - Social Engineering Attack Protection <p>After scanning the email message for suspicious files, URLs, and characteristics, Deep Discovery Email Inspector correlates the results to either assign a risk level and immediately execute a policy action based on the risk level, or send the file, URL and message samples to Virtual Analyzer for further analysis.</p> <p>Deep Discovery Analyzer is a secure virtual environment that manages and analyzes</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>SI-3 (10) System and Information Integrity / Malicious Code Protection / Malicious Code Analysis (... Continued.)</p>		<p>objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match the system configuration. Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:</p> <ul style="list-style-type: none"> - Anti-security and self-preservation - Autostart or other system configuration - Deception and social engineering - File drop, download, sharing, or replication - Hijack, redirection, or data theft - Malformed, defective, or with known malware traits - Process, service, or memory object change - Rootkit, cloaking - Suspicious network or messaging activity <p>During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC files that can be used in investigations.</p> <p>Deep Security supports this requirement through real-time, scheduled, and on-demand scans for file-based viruses and malware based upon known signatures. Deep Security performs scheduled scans at the time and frequency configured by the authorized administrator. This functionality is supported by the Trend Micro Smart Protection Network for malware analysis, which provides a response to the continuous emergence of new threats. New threats are created at a rate of 1.5 every second, historically methods required virus signature files, which would then have to be delivered to the premises equipment. This caused network loads, memory usage, and system loads to gradually increase daily. The Trend Micro Smart Protection Network works by storing the information required for security countermeasures in a cloud database rather than on individual computers and Trend Micro then carries out updates and management via the cloud. Therefore, a long-term reduction in work and system loads produced by delivering virus signature files is eliminated while simultaneously providing greater security countermeasures.</p> <p>Tipping Point supports analysis of malicious code through the Security Management System (SMS). The SMS dashboard provides at-a-glance monitors with launch capabilities into the targeted management applications that provide global command and control of Tipping Point. Included in the SMS dashboard display are the following items:</p> <ul style="list-style-type: none"> - Entries for the top five filters triggered over the past hour in various categories; - A graph of triggered filters over the past 24 hours; - The health status of devices. <p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-3 (10):</p> <ul style="list-style-type: none"> Deep Discovery Inspector: <ul style="list-style-type: none"> FAV_ACT.1,EXT - Anti-Virus Requirements / Anti-Virus Actions FAV_ALR.1,EXT - Anti-Virus Requirements / Anti-Virus Alerts Deep Security: <ul style="list-style-type: none"> FAV_ACT.1,EXT Anti-Virus Requirements / Anti-Virus Actions FAV_ALR.1,EXT Anti-Virus Requirements / Anti-Virus Alerts TippingPoint: <ul style="list-style-type: none"> IDS_ANL_EXT.1 - IDS / IDS Analyzer

SI-4 System and Information Integrity / Information System Monitoring

<p>SI-4 System and Information Integrity / Information System Monitoring</p> <p>a. Monitor the system to detect:</p> <ol style="list-style-type: none"> 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; <p>b. Identify unauthorized use of the system through [Assignment: organization-defined</p>	<p>L M H</p>	<p>E P</p>	<p>Deep Discovery Inspector monitors the organization's information system to detect attacks and indicators of potential attack through the Advanced Threat Scan Engine using a combination of file-based detection scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks. Deep Discover detection engines deliver expanded APT detection capabilities, including a customizable virtual analyzer and updated inspection and correlation rules designed to</p>
---	--------------	------------	---

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>techniques and methods];</p> <p>c. Invoke internal monitoring capabilities or deploy monitoring devices:</p> <ol style="list-style-type: none"> 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; <p>d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;</p> <p>e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;</p> <p>f. Obtain legal opinion regarding system monitoring activities; and</p> <p>g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].</p> <p>Supplemental Guidance:</p> <p>System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at system boundaries. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capability is achieved through a variety of tools and techniques, including, for example, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software. The distribution and configuration of monitoring devices can impact throughput at key internal and external boundaries, and at other locations across a network due to the introduction of network throughput latency. Therefore, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include, for example, selected perimeter locations and near key servers and server farms supporting critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs and output from system monitoring serves as input to those programs. Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other credible sources of information. The legality of system monitoring activities is based on applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.</p> <p>Related Controls: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-14, CA-7, CM-3, CM-8, CM-11, IA-10, IR-4, PE-3, PM-12, PM-24, RA-5, SA-18, SC-7, SC-26, SC-31, SC-35, SC-36, SC-37, SI-3, SI-6, SI-7.</p> <p>References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.</p>	<p>CNSSI FedRAMP 800-82 ICS 800-171 CUI</p>	<p>detect malicious content, communication, and behavior during every stage of an attack sequence. Deep Discovery Inspector increases the level of monitoring provided whenever there is an indication of increased risk to the organization's operations and assets.</p> <p>Deep Discovery Email Inspector is designed to integrate into an existing anti-spam/antivirus network topology. Deep Discovery Email Inspector can act as a mail transfer agent in the mail traffic flow (MTA mode) or as an out-of-band appliance monitoring a network for cyber threats (BCC mode or SPAN/TAP mode). Whichever deployment method is chosen, Deep Discovery Email Inspector investigates email messages for suspicious file attachments, embedded links (URLs), and characteristics. If an email message exhibits malicious behavior, Deep Discovery Email Inspector can block the threat and notify security administrators about the malicious activity.</p> <p>After Deep Discovery Email Inspector scans an email message for known threats in the Trend Micro Smart Protection Network, it passes suspicious files and URLs to the Virtual Analyzer sandbox environment for simulation. Virtual Analyzer opens files, including password-protected archives and document files, and accesses URLs to test for exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics. After investigating email messages, Deep Discovery Email Inspector assesses the risk using multi-layered threat analysis. Deep Discovery Email Inspector calculates the risk level based on the highest risk assigned between the Deep Discovery Email Inspector email scanners and Virtual Analyzer. Deep Discovery Email Inspector acts upon email messages according to the assigned risk level and policy settings. Configure Deep Discovery Email Inspector to block and quarantine the email message, allow the email message to pass to the recipient, strip suspicious file attachments, redirect suspicious links to blocking or warning pages, or tag the email message with a string to notify the recipient. While Deep Discovery Email Inspector monitors your network f</p> <p>Deep Discovery Analyzer provides sandboxing as a centralized service which ensures optimized performance with a scalable solution able to keep pace with email, network, endpoint, and any additional source of samples. Custom sandboxing performs sandbox simulation and analysis in environments that match the desktop software configurations attackers expect in an organization's environment and ensures optimal detection with low false-positive rates. Broad file analysis examines a wide range of Windows executable, Microsoft Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing. YARA rules are used to identify malware. YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to an organization's environment. Document exploit detection using specialized detection and sandboxing, discovers malware and exploits that are often delivered in common office documents and other file formats. Automatic URL Analysis performs page scanning and sandbox analysis of URLs that are automatically submitted by integrating products. Detailed reporting delivers full analysis results including detailed sample activities and C&C communications via central dashboards and reports. Alert notifications provide immediate intelligence about the state of Deep Discovery Analyzer. Custom defense integration shares new IOC detection intelligence automatically with other Trend Micro solutions and third-party security products.</p>
<p>SI-4 System and Information Integrity / Information System Monitoring</p> <p>(Continued: Deep Security)</p>		<p>Deep Security supports and satisfies this requirement through the Intrusion Prevention module which inspects incoming and outgoing traffic to detect and block suspicious activity. This prevents exploitation of known and zero-day vulnerabilities. Deep Security supports "virtual patching": Intrusion Prevention can be used with rules to shield from known vulnerabilities until they can be patched, which is required by many compliance regulations. Deep Security can be configured to automatically receive new rules that shield newly discovered vulnerabilities within hours of their discovery. The Intrusion Prevention module also protects web applications and the data that they process from SQL injection attacks, cross-site scripting attacks, and other web application vulnerabilities until code fixes can be completed. Other modules that support compliance with SI-4 are:</p> <ul style="list-style-type: none"> - Anti-Malware module protects Windows and Linux workloads against malicious software, such as malware, spyware, and Trojans. Powered by the Smart Protection Network, this module helps to instantly identify and remove malware and blacklist domains known to be command and control servers. - Firewall Module controls incoming and outgoing traffic and maintains firewall event logs for audits. - Web Reputation module provides content filtering by blocking access to malicious domains and known C&C servers used by criminals. This module taps into the Smart Protection Network, which identifies new threats quickly and accurately.

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
		<ul style="list-style-type: none"> - <u>Integrity Monitoring module</u> tracks both authorized and unauthorized changes made to an instance and enables an organization to receive alerts about unplanned or malicious changes. The ability to detect unauthorized changes is a critical component in a cloud security strategy, it provides visibility into changes that could indicate the compromise of an instance. - <u>Log Inspection module</u> captures and analyzes system logs to provide audit evidence for requirements that an organization may have. It helps to identify important security events that may be buried in multiple log entries. Log Inspection can be configured to forward suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving. - <u>Application Control module</u> monitors changes — “drift” or “delta” — compared to the computer’s original software. Once application control is enabled, all software changes are logged and events are created when it detects new or changed software on the file system. When Deep Security Agent detects changes, an organization can allow or block the software, and optionally lock down the computer.
SI-4 System and Information Integrity / Information System Monitoring (Continued: TippingPoint)		<p>TippingPoint is a high-speed, security system that includes the Intrusion Prevention System (IPS), Local Security Manager (LSM), Digital Vaccine, the Security Management System Appliance, and the Core Controller. TippingPoint’s security system provides a single, integrated, adaptive security system that includes hardware and a management interface. The SMS Server is an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices. The SMS provides the following functionality:</p> <ul style="list-style-type: none"> - Enterprise-wide device status and behavior monitoring — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status. - IPS networking and configuration — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group. - Filter customization — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings. - Filter and software distribution — Monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS client. The SMS client and Central Management Server can distribute these packages according to segment group settings. <p>The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates.</p> <p>The TippingPoint Security Management System (SMS) client provides services and functions to monitor, manage, and configure the entire TippingPoint system. This client is a Java-based application installed and accessed on a computer running the appropriate operating system. Each user receives a specific user level with enhanced security measures to protect access and configuration of the system. The SMS client can be installed on computers with Microsoft Windows, Mac, or Linux operating systems. The SMS features a policy-based operational model for scalable and uniform enterprise management. It enables behavior and performance analysis with trending reports, correlation and real-time graphs. Reporting includes all, specific, and top attacks and their sources and destinations, as well as all, specific, and top peers and filters for misuse and abuse (peer-to-peer piracy) attacks. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. An organization can modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention. The SMS dashboard provides at-a-glance monitors with launch capabilities into the targeted management applications that provide global command and control of TippingPoint. Included in the SMS dashboard display are the following items:</p> <ul style="list-style-type: none"> - Entries for the top five filters triggered over the past hour in various categories - A graph of triggered filters over the past 24 hours - The health status of devices - Update versions for software of the system <p>Through the Dashboard, an organization can gain an overview of the current performance of your system, including notifications of updates and possible issues with devices monitored by the SMS.</p>

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy
SI-4 System and Information Integrity / Information System Monitoring (Continued: Common Criteria evaluation)				<p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4:</p> <ul style="list-style-type: none"> Deep Discovery Inspector: <ul style="list-style-type: none"> FAV_ACT.1,EXT - Anti-Virus Requirements / Anti-Virus Actions FAV_SCN.1,EXT - Anti-Virus Requirements / Anti-Virus Scanning IDS_SDC.1, EXT - IDS Requirements / System Data Collection IDS_STG.1, EXT - IDS Requirements / Guarantee of System Data Availability Deep Security: <ul style="list-style-type: none"> FAV_ACT.1,EXT - Anti-Virus Requirements / Anti-Virus Actions FAV_SCN.1,EXT - Anti-Virus Requirements / Anti-Virus Scanning IDS_SDC.1, EXT - IDS Requirements / System Data Collection IDS_STG.1, EXT - ISD Requirements / Guarantee of System Data Availability TippingPoint: <ul style="list-style-type: none"> IDS_SDC_EXT.1 - IDS / IDS Data Collection IDS_STG_EXT.1 - IDS / IDS Data Storage
SI-4 (1) System and Information Integrity / Information System Monitoring / System -Wide Intrusion Detection System Connect and configure individual intrusion detection tools into a system-wide intrusion detection system. Supplemental Guidance: CM-6.	CNSSI FedRAMP 800-171 CUI	E		<p>Trend Micro Control Manager supports this requirement by providing the ability to configure and manage the IDS features across all Trend Micro products including Deep Security and Deep Discovery.</p> <p>Deep Discovery Inspector and Trend Micro Control Manager can send suspicious objects to TippingPoint SMS. To align with Control Manager, Deep Discovery Inspector sends each suspicious object with the following optional information:</p> <ul style="list-style-type: none"> Risk level: Severity of each suspicious object or C&C callback attempt Product Name: Trend Micro Deep Discovery Inspector Appliance Host Name: Trend Micro Deep Discovery Inspector host name <p>TippingPoint Security Management System (SMS) uses reputation filters to apply block, permit, or notify actions across an entire reputation group.</p>
SI-4 (2) System and Information Integrity / Information System Monitoring / Automated Tools for Real-Time Analysis Employ automated tools and mechanisms to support near real-time analysis of events. Supplemental Guidance: Automated tools and mechanisms include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or Security Information and Event Management technologies that provide real time analysis of alerts and notifications generated by organizational systems.	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E		<p>See the response to SI-4</p> <p>—</p> <p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (2):</p> <ul style="list-style-type: none"> TippingPoint: <ul style="list-style-type: none"> ISD_ANL_EXT.1 – IDS/ IDS Analyzer
SI-4 (3) System and Information Integrity / Information System Monitoring / Automated Tool and Mechanism Integration Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms. Supplemental Guidance: Using automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms facilitates a rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.	800-171 CUI	E P		<p>See response to SI-4</p> <p>In addition:</p> <p>Tipping Point provides automated tool and mechanism integration through the Threat Suppression Engine (TSE) a line-speed hardware engine that contains all the functions needed for Intrusion Prevention, including:</p> <ul style="list-style-type: none"> - IP defragmentation; - TCP flow reassembly; - Statistical analysis; - Traffic shaping; - Flow blocking; - Flow state tracking; - Application-layer parsing of over 170 network protocols. <p>The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious</p>

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy
SI-4 (3) System and Information Integrity / Information System Monitoring / Automated Tool and Mechanism Integration (... Continued.)				<p>traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The blocking of the traffic and packets ensures that the attack never reaches its destination.</p> <p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (3):</p> <p>TippingPoint: ISD_ANL_EXT.1 – IDS/ IDS Analyzer</p>
SI-4 (4) System and Information Integrity / Information System Monitoring /Inbound and Outbound Communications Traffic Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions. Supplemental Guidance: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational systems or propagating among system components; the unauthorized exporting of information; or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components.	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P		<p>See response to SI-4</p> <p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (4):</p> <p>Deep Discovery Inspector: IDS_SDC.1,EXT - IDS Requirements / System Data Collection</p> <p>Deep Security: IDS_SDC.1,EXT - IDS Requirements / System Data Collection</p> <p>TippingPoint: IDS_SDC_EXT.1 - IDS / IDS Data Collection</p>
SI-4 (5) System and Information Integrity / Information System Monitoring / System - Generated Alerts Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators]. Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated or they may be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include, for example, system administrators, mission or business owners, system owners, system security officers, or privacy officers. This control enhancement focuses on the security alerts generated by the system. Alternatively, alerts generated by organizations in SI-4(12) focus on information sources external to the system such as suspicious activity reports and reports on potential insider threats. Related Controls: AU-4, AU-5, PE-6.	M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E P		<p>See response to SI-4</p> <p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (5):</p> <p>Deep Discovery Inspector: IDS_RCT.1,EXT - IDS Requirements / Analyser Reacts</p> <p>Deep Security: IDS_RCT.1,EXT - IDS Requirements / Analyser React</p> <p>TippingPoint: IDS_RCT_EXT.1 – IDS / IDS Intrusion Reaction</p>
SI-4 (7) System and Information Integrity / Information System Monitoring / Automated Response to Suspicious Events Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events and take [Assignment: organization-defined least-disruptive actions to terminate suspicious events]. Supplemental Guidance: Least-disruptive actions include, for example, initiating requests for human responses.	800-171 CUI	E P		<p>See response to SI-4</p> <p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p>
SI-4 (9) System and Information Integrity / Information System Monitoring / Testing of Monitoring Tools Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency]. Supplemental Guidance: Testing intrusion-monitoring tools and mechanism is necessary to ensure that the tools and mechanisms are operating correctly and continue to satisfy the monitoring objectives	800-171 CUI			<p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (7):</p> <p>Deep Discovery Inspector: IDS_RCT.1,EXT - IDS Requirements / Analyser Reacts</p> <p>Deep Security: IDS_RCT.1,EXT - IDS Component Requirements / Analyser React</p>

NIST SP 800-53 r5 Control	Baseline Context	Trend Micro Solution Compliancy
<p>of organizations. The frequency of testing depends on the types of tools and mechanisms used by organizations and the methods of deployment.</p> <p>Related Controls: CP-9.</p>		
<p>SI-4 (11) System and Information Integrity / Information System Monitoring / Analyze Communications Traffic Anomalies</p> <p>Analyze outbound communications traffic at the external boundary of the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.</p> <p>Supplemental Guidance: Examples of organization-defined interior points within the system include subnetworks and subsystems. Anomalies within organizational systems include, for example, large file transfers; long-time persistent connections; unusual protocols and ports in use; and attempted communications with suspected malicious external addresses.</p>	CNSSI FedRAMP 800-171 CUI	<p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (11):</p> <p>Deep Discovery Inspector: IDS_ANL.1,EXT - IDS Requirements / Analyser Analysis</p> <p>Deep Security: IDS_ANL.1,EXT - IDS Requirements / Analyser Analysis</p> <p>TippingPoint IDS_SDC_EXT.1 – IDS / Data Collection</p>
<p>SI-4 (12) System and Information Integrity / Information System Monitoring / Automated Alerts</p> <p>Employ automated mechanisms to alert [Assignment: organization-defined personnel or roles] when the following organization-generated indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].</p> <p>Supplemental Guidance: Organizational personnel on the alert notification list can include, for example, system administrators, mission or business owners, system owners, system security officers, or privacy officers. This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by systems in SI-4(5) that focus on information sources that are internal to the systems such as audit records, the sources of information for this enhancement focus on other entities such as suspicious activity reports and reports on potential insider threats.</p>	CNSSI 800-171 CUI	<p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (12):</p> <p>Deep Discovery Inspector: IDS_RCT.1,EXT - IDS Requirements / Analyser Reacts</p>
<p>SI-4 (13) System and Information Integrity / Information System Monitoring / Analyze Traffic / Event Patterns</p> <p>(a) Analyze communications traffic and event patterns for the system; (b) Develop profiles representing common traffic and event patterns; and (c) Use the traffic and event profiles in tuning system-monitoring devices to reduce the number of false positives and false negatives.</p>	800-171 CUI	<p>E P</p> <p>See response to SI-4</p> <p>Common Criteria Security Targets include “extended functions” which are security requirements not found in the Common Criteria. The “extensions” in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements.</p> <p>The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (13):</p> <p>Deep Discovery Inspector: IDS_ANL.1,EXT - IDS Requirements / Analyser Analysis</p> <p>Deep Security: DS_ANL.1,EXT - IDS Requirements / Analyser Analysis</p>
<p>SI-4 (15) System and Information Integrity / Information System Monitoring / Wireless to Wireline Communications</p> <p>Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.</p> <p>Related Controls: AC-18.</p>	CNSSI 800-171 CUI	<p>E</p> <p>Deep Security Firewall rules for wireless partially support compliance to this requirement. With many devices now capable of connecting to both the wired and wireless networks, users need to be aware of the problems that can result from this scenario. The common problem is a “network bridge” configured between the wired and wireless network. There is a risk of forwarding the internal traffic externally and potentially expose internal hosts to external attacks. Deep Security allows administrators to configure a set of firewall rules for these types of users to prevent them from creating a network bridge.</p>
<p>SI-4 (18) System and Information Integrity / Information System Monitoring / Analyze Traffic / Covert Exfiltration</p> <p>Analyze outbound communications traffic at the external boundary or perimeter of the system and at [Assignment: organization-defined interior points within the system] to detect covert exfiltration of information.</p> <p>Supplemental Guidance: Examples of organization-defined interior points within the system include subnetworks and subsystems. Covert means that can be used for the exfiltration of information include, for example, steganography.</p>	FedRAMP 800-171 CUI	<p>E</p> <p>See response to SI-4</p>

NIST SP 800-53 r5 Control		Baseline	Context	Trend Micro Solution Compliancy
SI-4 (23) System and Information Integrity / Information System Monitoring / Host-Based Devices Implement [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined system components]. Supplemental Guidance: System components where host-based monitoring can be implemented include, for example, servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors. Related Controls: AC-18, AC-19.	CNSSI FedRAMP 800-171 CUI	E	See response to SI-4	
SI-4 (24) System and Information Integrity / Information System Monitoring / Indicators of Compromise Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise. Supplemental Guidance: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs for the discovery of compromised hosts can include, for example, the creation of registry key values. IOCs for network traffic include, for example, Universal Resource Locator or protocol elements that indicate malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack. Related Controls: AC-18.	FedRAMP 800-171 CUI	E P	See response to SI-4 Common Criteria Security Targets include “ extended functions ” which are security requirements not found in the Common Criteria. The “ extensions ” in the CC evaluation requirements for Deep Discovery Inspector, Deep Security and TippingPoint are related to (1) Anti-virus Requirements and (2) Intrusion Detection System Requirements. The CC evaluations of the following extensions assist in demonstrating compliance to SI-4 (24) : Deep Discovery Inspector: DS_RCT.1,EXT - IDS Requirements / Analyser Reacts Deep Security: DS_RCT.1,EXT - IDS Requirements / Analyser Reacts	

SI-5 System and Information Integrity / Security Alerts, Advisories and Directives

SI-5 System and Information Integrity / Security Alerts, Advisories, and Directives a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance. Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission or business partners, supply chain partners, external service providers, and other peer or supporting organizations. Related Controls: PM-15, RA-5, SI-2. References: NIST Special Publication 800-40.	L M H CNSSI FedRAMP 800-82 ICS 800-171 CUI	E	Deep Discovery Inspector and Deep Security can assist in supporting this control by providing security alerts to the organization through the Trend Micro Control Manager and security alert data can be exported to syslog servers. The frequency of alerts is configurable by the Deep Discovery Inspector Administrator. Other services provided by Trend Micro also effectively supports compliance with these controls: - Smart Protection Network; - TrendLabs; - Control Manager; and - Threat Management Services Portal. The Smart Protection Network uses a global network of threat intelligence sensors to continually update email, web, and file reputation databases in the cloud, identifying alerting, and blocking threats in real time before they reach the organization requiring the protection.
SI-5 (1) System and Information Integrity / Security Alerts, Advisories, and Directives / Automated Alerts and Advisories Employ automated mechanisms to make security alert and advisory information available throughout the organization. Supplemental Guidance: The significant number of changes to organizational systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three tiers related to	H CNSSI FedRAMP 800-82 ICS 800-171 CUI		TrendLabs is the Trend Micro global infrastructure of antivirus research and product support centers that provide up-to-the-minute security information to Trend Micro customers. The “virus doctors” at TrendLabs monitor potential security risks around the world to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements. TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support 24x7. TrendLabs’ has earned ISO 9002 certification for its quality management procedures —one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry. Trend Micro Control Manager supports this requirement by automating the distribution and reporting of alerts and security incidents detected by Deep Security and Deep Discovery Inspector throughout the organization. The Trend Micro Threat Management Services Portal (TMSP) builds intelligence about an organizations network by providing meaningful reports at the executive or administrative level. Administrative-level reports keep IT security personnel

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
the management of information security and privacy risk including the governance level, mission and business process level, and the system level.			informed about the latest threats and provide action items that help defend the network from these threats. Executive-level reports inform key security stakeholders and decision makers about the networks overall security posture, allowing them to fine tune security policies and strategies to address the latest threats.
SI-7 System and Information Integrity / Software, Firmware and Information Integrity			
SI-7 System and Information Integrity / Software, Firmware, and Information Integrity Employ integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information]. Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes personally identifiable information and metadata containing security and privacy attributes associated with information. Integrity-checking mechanisms including, for example, parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools can automatically monitor the integrity of systems and hosted applications. Related Controls: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-9, SA-10, SA-18, SA-19, CM-7, SA-12, SC-8, SC-13, SC-28, SC-37, SI-3. References: FIPS Publications 140-2, 180-4, 186-4, 202; NIST Special Publications 800-70, 800-147.	M H CNSSI FedRAMP 800-82 ICS	E	See response to SI-4
SI-7 (1) System and Information Integrity / Software, Firmware, and Information Integrity / Integrity Checks Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]]. Supplemental Guidance Security-relevant events include, for example, the identification of a new threat to which organizational systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.	M H CSSSI FedRAMP 800-82 ICS		
SI-7 (3) System and Information Integrity / Software, Firmware, and Information Integrity / Centrally Managed Integrity Tools Employ centrally managed integrity verification tools. Related Controls: AU-3, SI-2, SI-8.			
SI-7 (5) System and Information Integrity / Software, Firmware, and Information Integrity / Automated Response to Integrity Violations Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined security safeguards]] when integrity violations are discovered. Supplemental Guidance: Organizations may define different integrity checking responses by type of information, by specific information, or a combination of both. Examples of types of information include firmware, software, and user data. Examples of specific information include boot firmware for certain types of machines. The automatic implementation of safeguards within organizational systems includes, for example, reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.	H CNSSI FedRAMP 800-82 ICS		
SI-7 (8) System and Information Integrity / Software, Firmware, and Information Integrity / Auditing Capability for Significant Events Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]]. Supplemental Guidance: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations. Related Controls: AU-2, AU-6, AU-12.	CNSSI		

NIST SP 800-53 r5 Control	Baseline	Context	Trend Micro Solution Compliancy
<p>SI-7 (13) System and Information Integrity / Software, Firmware, and Information Integrity / Code Execution In Protected Environments</p> <p>Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is:</p> <ul style="list-style-type: none"> (a) Obtained from sources with limited or no warranty; and/or (b) Without the provision of source code. <p>Supplemental Guidance:</p> <p>This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software and firmware and open source software.</p> <p>Related Controls: CM-10, SC-44.</p>		E	<p>Deep Discovery Analyzer can deploy a Sandbox Image which is a template used to deploy sandbox instances. A sandbox image includes an operating system, installed software, and other settings necessary for that specific computing environment. This is considered to be a protected environment for execution of binary or machine-executable code. Sandbox images allow observation of file (binary or executable) and network behavior in an environment without any risk of compromising the network. Virtual Analyzer performs static analysis and behavior simulation to identify potentially malicious characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings. Use standalone sandboxing capability.</p>